VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Monitorování hrozeb Wi-Fi sítí za pomocí Honeypot
Threats Monitoring in Wi-Fi networks using Honeypot

2012 **Bc. Tomáš Měrka**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Tomáš Měrka**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Monitorování hrozeb Wi-Fi sítí za pomocí Honeypot
Threats Monitoring in Wi-Fi networks using Honeypot

Zásady pro vypracování:

Bezpečnost bezdrátových sítí standardu 802.11 je v současné době aktuálním problémem. Veřejné či soukromé Access Pointy jsou často cílem útoků za účelem získat přístup do distribuované sítě, či jinak tuto síť penetrovat. Cílem diplomové práce je implementovat a provozovat tzv. testovací Wi-Fi Honeypot, který bude v několika destinacích s vysokou intenzitou provozu sloužit jako monitorovací prostředí pro příchozí útoky. Ty mohou být generovány uměle pomocí série penetračních testů, nebo se bude jednat o útoky z reálného prostředí. Následnou analýzou budou definovány nejčastěji používané typy hrozeb a budou vytvořeny praktická protiopatření, která by útoky v praxi omezila, či úplně eliminovala.

1. Studijní část: Wi-fi, bezpečnostní algoritmy a jejich využití ve standardu 802.11
2. Detailní přehled nástrojů pro implementaci 802.11 Honeypot
3. Praktická implementace Wi-Fi Honeypot
4. Statistika útoků z reálného a testovaného prostředí
5. Teoretický návrh pravidel a algoritmů pro omezení a eliminaci hrozeb
6. Praktická implementace navržených metod zabezpečení

Seznam doporučené odborné literatury:

BackTrack 5 Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran (Sep 9, 2011)

Honeypots: A New Paradigm to Information Security by R. C. Joshi and Anjali Sardana (Feb 3, 2011)

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Filip Řezáč**

Datum zadání: 18.11.2011

Datum odevzdání: 04.05.2012

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky OSTRAVA

prof. RNDr. Vladimír Vašinek, CSc.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Dne: 4. 5. 2012

…….

Podpis zástupce

Poděkování

Rád bych poděkoval Ing. Filipu Řezáčovi za odbornou pomoc a konzultaci při tvorbě diplomové práce.

Prohlášení zástupce spolupracující právnické nebo fyzické osoby

„Souhlasím se zveřejněním této bakalářské/diplomové práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských/magisterských programech VŠB-TU Ostrava.“

Dne: 4. 5. 2012 …….

Podpis zástupce

Abstrakt

Bezpečnost bezdrátových sítí standardu 802.11 je v současné době aktuálním problémem. Veřejné či soukromé Access Pointy jsou často cílem útoků za účelem získat přístup do distribuované sítě, či jinak tuto síť penetrovat. Cílem diplomové práce je implementovat a provozovat tzv. testovací Wi-Fi Honeypot, který bude v několika destinacích s vysokou intenzitou provozu sloužit jako monitorovací prostředí pro příchozí útoky. Ty mohou být generovány uměle pomocí série penetračních testů, nebo se bude jednat o útoky z reálného prostředí. Následnou analýzou budou definovány nejčastěji používané typy hrozeb a budou vytvořena praktická protiopatření, která by útoky v praxi omezila, či úplně eliminovala.

Klíčová slova

Wi-Fi, Honeypot, Honeyd, KFSensor, IDS, bezpečnost, WEP, WPA, 802.11,

Abstract

Security of 802.11 wireless networks is now the current problem. Public or private access points are often the target of attacks in order to gain access to a distributed network, or otherwise penetrate the network. The aim of this thesis is to implement and operate the test Wi-Fi honeypot, which will in a few destinations with lots of traffic to serve as a monitoring environment for incoming attacks. These can be generated artificially by using a series of penetration tests, or it will be a real-world attacks. The subsequent analysis will be defined most commonly used types of threats and countermeasures will be made practical, attacks that would in practice limit, or completely eliminated.

Key words

Wi-Fi, a honeypot, Honeyd, KFSensor, IDS, security, WEP, WPA, 802.11,

Seznam použitých zkratek

Zkratka	Anglický význam
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
CDMA	Code Division Multiple Access
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Systém
DoS	Denial of Service
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
FTP	File Transfer Protoco
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
CHAP	Challenge-handshake authentication protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IV	Initialization vector
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NAS	Network Access Server
OS	Operating System
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Service
RFC	Request for Comments
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
VPN	Virtual private network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

Obsah

1 Úvod

S pojmem bezdrátových sítí se v současné době setkáváme stále častěji. Pro firmy i domácí uživatelé jsou velice lákavé, protože poskytují vynikající míru mobility a svobody. Hlavní odlišnost bezdrátových Wi-Fi sítí od jiných technologií (např. GSM, CDMA) tkví ve využití bezlicenčního frekvenčního pásma. Wi-Fi je podceňovanou technologií, protože není kladen důraz uživatelů na její zabezpečení. Z hlavního důvodu, že je využívána, jako propojovací technologie. Což je sice pravda, ale musíme si uvědomit, že má svá specifika, která nesou řadu rizik. Nejen, že se útočník může dostat k posílaným datům, ale může využívat třeba naše Wi-Fi připojení k dostupnosti sítě Internet. Často tak činní, aby konal činnosti neetické či rovnou nelegální, čímž nás poškozuje jak technicky, tak i na dobré pověsti. Dále může útočník tímto způsobem např. zavést škodlivý software do vnitřního systému. Bezpečnost bezdrátových sítí standardu 802.11 je v současné době aktuálním problémem. Veřejné či soukromé Access Pointy jsou často cílem útoků za účelem získáni přístupu do distribuované sítě, či jinak tuto síť penetrovat. Z těchto důvodu je nutné vědět, jakými způsoby útočníci pronikají do bezdrátových sítí. Cílem práce je vytvoření bezdrátového Honeypotu, který nám bude zaznamenávat případné útoky v reálném a testovaném prostředí. V první kapitole se zabývám popisem současného zabezpečení bezdrátových sítí. Druhá kapitola popisuje nástroje pro vytvoření Honeypotu k naším účelům, na kterou navazuje třetí, kde tyto nástroje prakticky implementuji. Čtvrtá kapitola zobrazuje statistiku zmíněných útoku na bezdrátovou síť. Pátá a šestá kapitola navazuje na předchozí, kde jsem se zabýval způsobem, jak více zabezpečit bezdrátovou infrastrukturu před případnými útoky.

„Učit se znamená objevovat to, co už víš.

Konat znamená demonstrovat, že to víš.

Učit druhé znamená připomínat jim, že to vědí stejně dobře jako ty.

Všichni jste zároveň žáci, praktikanti a učitelé. “

Richard Bach

2 Wi-fi, bezpečnostní algoritmy

2.1 Bezdrátové sítě

Mnoho uživatelů bezdrátových sítí si myslí, že koupením vhodného Access Pointu (AP, přístupového bodu) a bezdrátové karty vše končí. Ale je důležité si uvědomit různé rizika bezdrátových sítí a vnitřní fungování celé topologie.

2.2 Bezpečnostní faktory

Dnes se primární faktory, které definují bezpečnost v bezdrátových sítích, soustředí do pěti bodů, které jsou vzájemně závislými komponentami.

1. Odcizení
2. Řízení přístupu
3. Ověřování
4. Šifrování
5. Bezpečnostní opatření

2.2.1 Odcizení

Neoprávněný uživatel se často pokouší přihlásit do podnikové sítě a ukrást údaje za účelem dosažení zisku. Také propuštění zaměstnanci často cítí nelibost proti bývalému zaměstnavateli a snaží se zmocnit podnikových dat před tím, než opustí své pracovní místo. [5]

2.2.2 Řízení přístupu

Bezdrátové sítě mají všechny neduhy zranitelnosti řízení přístupu jako kabelové sítě, ale mohou být snadno napadnutelné a přístupné zvenčí. Nejběžnějším typem útoku je usednout poblíž kancelářské budovy a pomocí počítače s bezdrátovou kartou zkoušet všechny dostupné 802.11 sítě.

Většina uživatelů si nenastaví ani ty nejjednodušší metody zabezpečení, které brání v přístupu cizího uživatele do sítě a odcizení soukromých. [5]

2.2.3 Ověřování

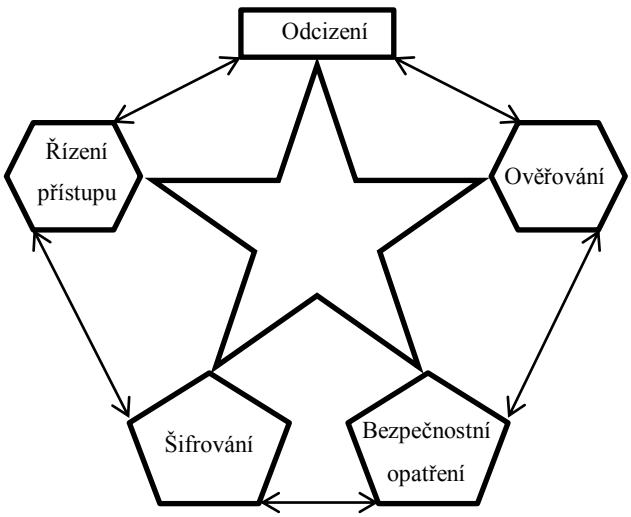
Když se uživatel přihlásí, nemůžeme říct, zda přihlášená osoba je majitel účtu. Běžnou praxí je, že lidé používají k přihlášení účty jiných osob. Ve většině domácích i podnikových sítí je nastaven jen jeden účet. Problém je v tom, že útočník se může snadno přihlásit do této sítě a správce nerozezná, zda se jedná o oprávněného uživatele. [5]

2.2.4 Šifrování

Pokud útočník není schopen přímo se přihlásit do sítě, může použít tzv. "Packet sniffer"[1], aby se pokusil odposlouchávat provoz na síti. Tímto způsobem se útočník nemůže autentizovat do vaší sítě, ale stále je schopen ukrást citlivé data monitorováním vašeho provozu. Pomocí tzv. “sniffingu” může získat uživatelské jména, hesla a další soukromé informace.

2.2.5 Bezpečnostní opatření

Nejlepší ochranou je seznámit se s možnostmi vašeho AP. Dále vytvořit dostačující šifrovací klíč o velikosti minimálně 128 bit. Je nutné si však uvědomit, že některé starší karty podporují pouze nižší úroveň šifrování. Proto je vhodné investovat do zakoupení nové síťové karty. [5]



Obrázek 2.1: Bezpečnostní faktory

[1] Packet sniffer nástroj pro zachytávání paketů a analýzu síťových protokolů

2.3 Základy zabezpečení AP

2.3.1 SSID

SSID (Service Set Identifier) je jedinečný identifikátor každé bezdrátové sítě. Přístupový bod (AP) vysílá tento identifikátor v pravidelných intervalech v takzvaném majákovém rámci (beacon frame). Klienti si tak mohou vybrat, ke kterému bodu se přihlásí.

SSID se skládá z ASCII řetězce dlouhého 32 znaků. Tento parametr představuje klíč, kterým dochází ke spojení jednotlivých adaptérů v rámci bezdrátové sítě. Všechna bezdrátová zařízení pokoušející se o vzájemnou komunikaci mezi sebou musí předávat ten samý SSID.

Administrátoři často používají veřejné SSID, které vysílá ke všem bezdrátovým zařízením ve svém rozsahu. Z důvodu větší bezpečnosti se doporučuje vysílání SSID vypínat. Současné novější bezdrátové přístupové body zablokují automatickou volbu vysílání SSID s cílem zlepšit zabezpečení.

Pokročilé AP dnes podporují vysílání mnohanásobných SSID, které poskytujících vytváření virtuálních AP.

Dnes již útočník má k dispozici řadu programů pro zjištění vaší SSID i když jsou skryté. Tyto programy existují pro různé platformy operačních systému.

NetStumbler a *MiniStumbler* pro OS Windows, *Kismet, WEPCrack, AirSnort, THC-RUT, PrismStumbler* pro systémy Linux. Dokonce i pro Mac OS existuje program a tím je *MacStumbler*. [6][1]

2.3.2 WEP protokol

WEP (Wired Equivalent Privacy) byl výchozím šifrovacím protokolem, který byl poprvé uveden v roce 1999 ve standardu IEEE 802.11. Je založen na principu šifrovacího algoritmu RC4 s tajným klíčem o velikosti 40 nebo 104 bitů kombinovaným s 24 bitových inicializačním vektorem (IV) pro šifrování textové zprávy. Klíčem k bezpečnosti WEP je samozřejmě inicializační vektor, takže k udržení přiměřené úrovně zabezpečení a zmenšení možnosti odhalení by měl být IV zvětšen pro každý paket tak, aby se následné pakety šifrovaly odlišnými klíči. Bohužel v protokolu WEP se IV přenáší jako nešifrovaný text a standard 802.11 nenařizuje zvyšování IV, proto je toto bezpečnostní opatření ponecháno na volbě jednotlivých implementacích bezdrátových terminálů.

Protokol WEP nebyl vytvořen odborníky na bezpečnost nebo kryptografii. Z tohoto důvodu rychle prokázal svou zranitelnost vůči problémům RC4.

Problémem WEP protokolu je často se opakující inicializační vektor. Z důvodu statického klíče útočník jednoduše nasbírá dostatečný počet paketů. Při dostatečném počtu dojde k opakování stejného iniciačního vektoru a tím umožní útočníkům šifru prolomit.

Proto protokol WEP poskytuje přijatelnou úroveň bezpečnosti pouze pro domácí uživatele a méně důležité aplikace. V roce 2004 zveřejnili útok KoreK, který dokáže dešifrovat libovolné pakety bez znalosti klíče pomocí injekce paketů. Nástroje k nabourávání systémů jako *Aircrack* od Christophe Devine nebo *WepLab* od José Ignacio Sánchez, jsou schopny dešifrovat 128bitový klíč WEP za méně než 10 minut.

Dnes je protokol WEP definitivně zastaralý a neměl by se používat ani s cyklickým posuvem klíčů. [6][4]

2.3.3 **802.11i**

V roce 2001 byl WEP považován za nedostatečný mechanismus pro WLAN, nesplňující současné požadavky na bezpečnost sítí, proto byla sestavena skupina za účelem zlepšení autentizace dat standardu 802.11 a bezpečnosti šifrování. V dubnu 2003 oznámila Wi-Fi Alliance řešení bezpečnosti a v roce 2004 bylo schváleno vydání standardu 802.11i, který dostal od asociace Wi-Fi Alliance komerční název WPA/WPA2.

Verze normy 802.11i se skládá z několika části. Objevují se zde dva nové zabezpečovací protokoly TKIP a CCMP. Využívá systém kontroly přístupu k síti, definovaného podle 802.1x. [6][12]

2.3.4 **TKIP (Temporal Key Integrity Protocol)**

Bezpečnostní protokol, který byl navržen pro lepší zabezpečení, než nedostačující původní WEP protokol. Mezi hlavní znaky patří průběžná a automatická výměna vytvářených klíčů. Toto řeší základní slabinu WEP technologie, kdy zabraňuje útočníkovy získat dostatečný počet dat šifrovaný stejným způsobem. [12]

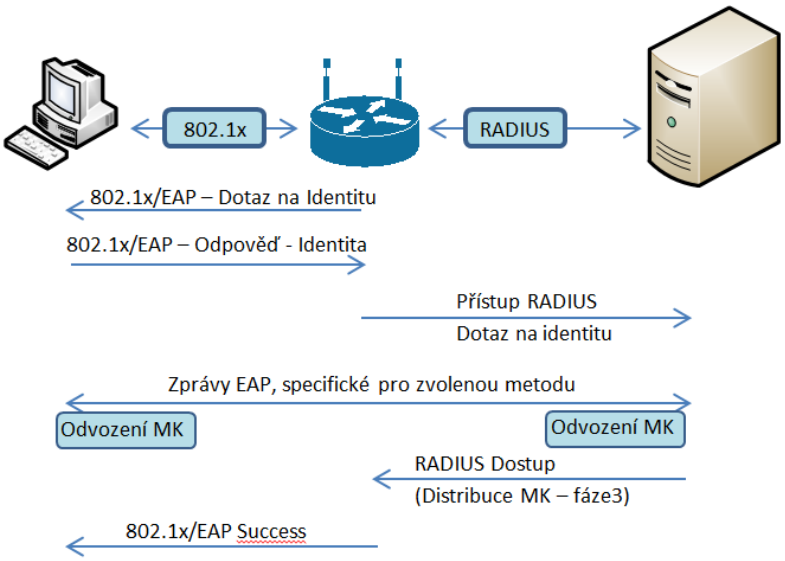
2.3.5 **CCMP (Temporal Key Integrity Protocol)**

TKIP funguje jen jako nástavba proto musel být definován bezpečnější protokol. CCMP je definován pro novější zařízení, které zajišťuje autentizaci i šifrování paketů. Oproti staršímu protokolu již využívá pro větší důvěryhodnost šifrování AES[2]. [12]

[2] Vyvinuta 2. ledna 1997, Joada Daemena a Vincenta Rijmena

2.3.6 IEEE 802.1x

Nástroj pro autentizaci a autorizaci zařízení pro připojení do sítě. Když se uživatel připojí na síťový port, má blokovanou veškerou komunikaci kromě EAP protokolu. Následuje fáze autentizace, kterou ověřovatel (authenticator, většinou switch) předává autentizačnímu serveru typicky RADIUS. Pokud dojde k úspěšné autentizaci, tak se port přepne do autorizovaného stavu. V bezdrátové síti přebírá roli ověřovatele AP a klient roli žadatele.



Obrázek 2.2: 802.1x komunikace

Postup připojení:

- Klient vyšle přes EAP protokol žádost o autentizaci na AP server.
- AP přepošle žádost RADIUS serveru.
- Jedná-li se o lokálního uživatele, ověření probíhá přímo na RADIUS serveru.
- O výsledku autentizace je informován AP, který síťový provoz povolí či zakáže. [6]

3 Přehled nástrojů pro implementaci 802.11 Honeypot

Bezdrátový Honeypot je jednoduchý bezdrátový bod, který čeká na útočníky nebo nepřátelské uživatele, kteří se snaží projít bezdrátovou infrastrukturou. Bezdrátový Honeypot může pomoci odhalit skutečné útoky na vaší síť a vytvářet statistiky, jako četnost útoků, úroveň dovedností útočníka, jeho cíle a metody. Může také pomoci s ochranou vaší sítě, zatímco útočník vynakládá velkou sílu na falešné cíle a jejich objevovaní v sítí. [10]

3.1 Potřeby a cíle bezdrátových Honeypots

Bezdrátové sítě jsou více náchylné k narušení bezpečností než jejich kabelové protějšky. Ethernetové LAN sítě jsou chráněny proti útočníkům ze své podstaty připojením tzn. útočník se musí pomocí metalického kabelu připojit do sítě, zatímco u Wi-Fi stačí, aby byl v přítomnosti zdroje signálu. Útočník může být v místnosti, mimo budovu nebo sedět v autě a parkovat stovky metrů od přístroje. Tento nedostatek nutnosti jakéhokoliv fyzického spojení umožňuje útočníkovi rychle a bezpečně uniknout.

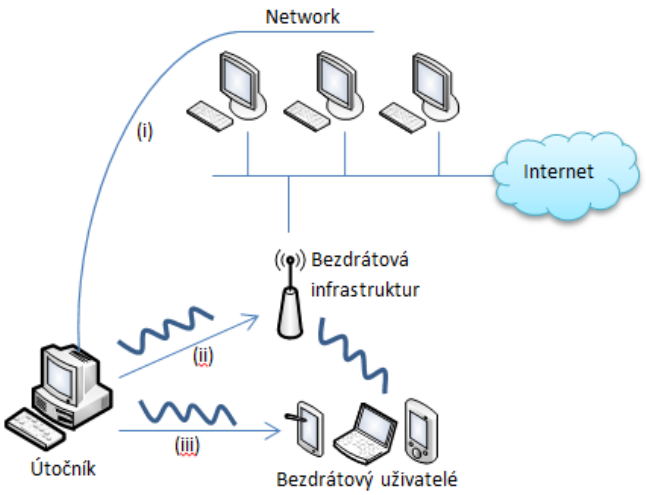
Stále je zde velký počet otevřených nebo nezabezpečených přístupových bodů (hotspoty[3] v hotelích, na letištích, veřejné prostory, SOHO[4] sítě atd.).

Pro korporátní útočníky a „cyber-teroristy“ je proniknutím do bezdrátové sítě snadný způsob, jak přistupovat k pevným zdrojům. Můžou libovolně používat otevřené AP a anonymně provádět útoky. Hlavním cílem Honeypotu je shromažďovat informace a vytvářet statistiky o reálných útocích, napadení síťové vrstvy, způsob útoku a použité techniky, četnost těchto útoků, úroveň dovedností útočníka, jeho cíle a metody. Bezdrátové Honeypoty pomáhají ke zjištění způsobu vniknutí do sítě a také díky falešným zdrojům zaneprázdňují útočníka. [3]

[3] Místo či oblast s možností bezdrátového připojení k internetu
[4] Malá domácí síť

3.2 Teorie a návrh

Když mluvíme o bezdrátové technologii a Honeypot, jsou tu tři různé scénáře útoku, které jsou znázorněné na obrázku.



Obrázek 3.1: Scénáře útoku

i. Útoky zaměřené na kabelové sítě, které bezdrátová síť spojuje. Tyto útoky používají bezdrátovou síť pouze jako médium, ale primárním cílem je síť nebo informační systémy za ním.
ii. Útoky směřující na infrastrukturu bezdrátové sítě. Tyto útoky se zaměřují na získání kontroly nad přístupovým bodem nebo na bezdrátovou infrastrukturu sítě.
iii. Útoky směřující na bezdrátové uživatele. Tyto útoky používají bezdrátovou síť jako prostředek k zaměření uživatelských zařízení a využití jejich funkcí. Využívají k tomu, že bezdrátové zařízení je zapnuto. Uživatel může nebo nemusí být připojení k bezdrátové síti. [3]

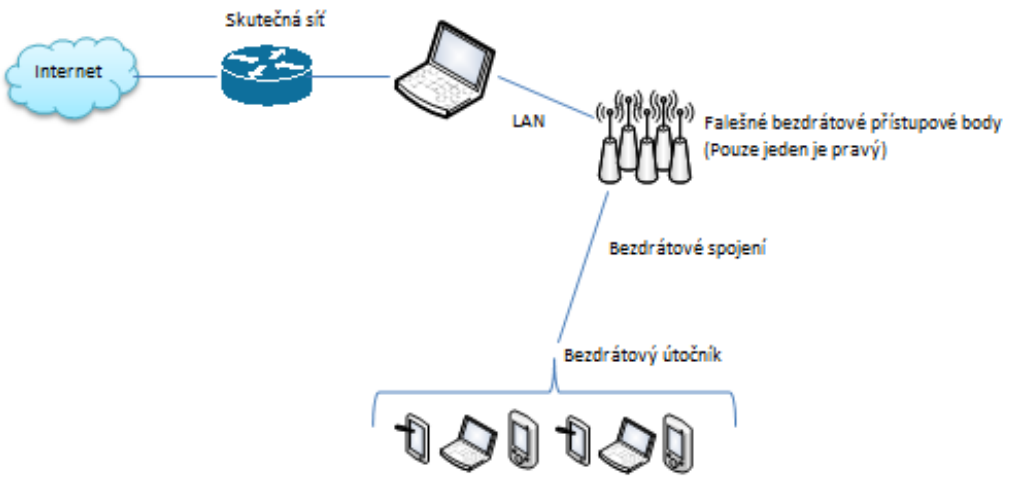
3.3 Bezdrátová architektura

V této části jsou popsány konkrétní nástroje pro realizaci Honeypotů, které lze použít v bezdrátovém prostředí podle rozličných typů útoků.

3.3.1 Architektura „Beacon“

Nejběžnější typy útoků se snaží zaměřit na otevřené sítě a využít jejich zranitelnosti. Přístupový bod vysílá signály, aby sdělil uživatelům svou přítomnost. Tento signál obsahuje SSID (Identifikátor síťové služby), čas, parametry fyzické vrstvy a podporované rychlosti přenosu dat. Tyto funkce mohou dopomoci útočníkovi zahájit útok proti síti.

Obrázek 3.2 ukazuje architekturu Honeypotu ve scénáři, kde je skutečná síť překryta simulováním mnoha falešnými sítěmi. Každá falešná síť vysílá svůj „Beacon“ ke zmatení útočníka.

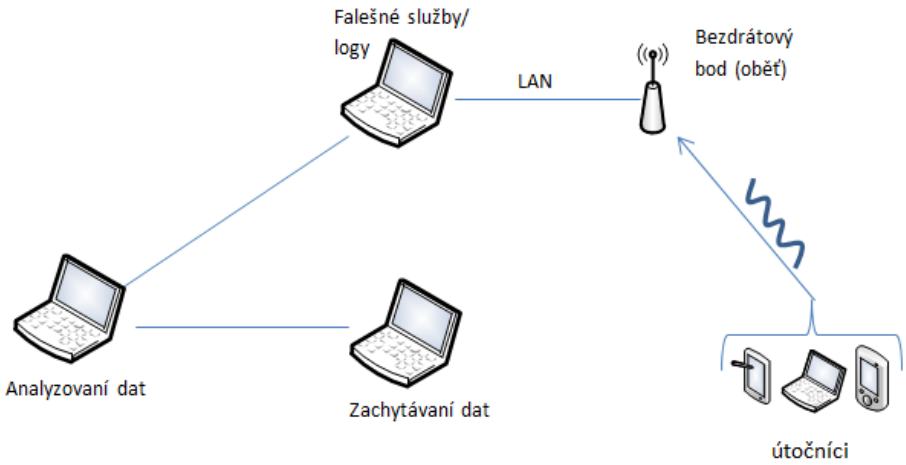


Obrázek 3.2: Architektura Beacon

Zaměřit se na jednu síť je snadný úkol, ale více cílů mate útočníka a je obtížné napadnout skutečným bezdrátový bod. [3]

3.3.2 Útoky na bezdrátový přístupový bod

Tato architektura se zabývá útoky, které jsou zaměřené na síťovou infrastrukturu. Tyto útoky jsou zaměřeny na získání kontroly nad přístupovým bodem. Útočník se snaží připojit k webovému rozhraní pomocí výchozího hesla, nebo se snaží získat přístup k dalším otevřeným službám (jako jsou: SNMP, DNS, DHCP, TFTP, atd.). Útočník se může pokusit využít přehlcení vyrovnávací paměti a zrušit bezdrátový přenos. [3]

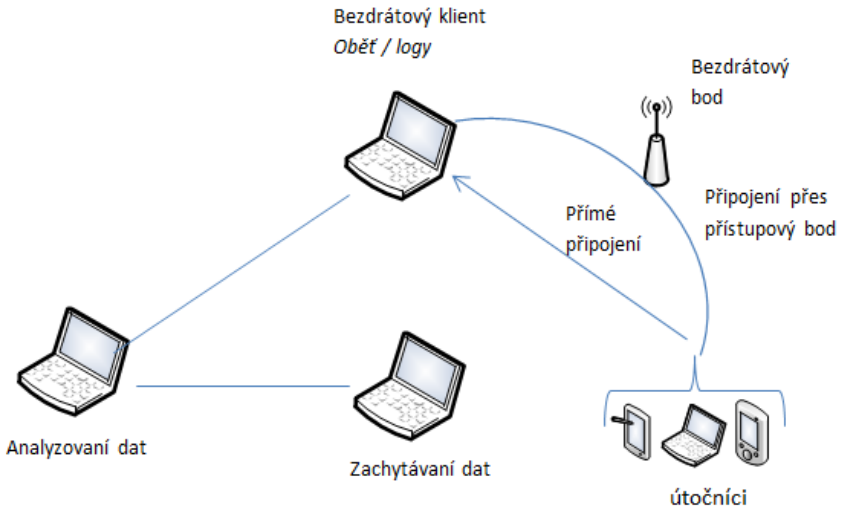


Obrázek 3.3: Útoky na bezdrátový bod

3.3.3 Útoky směřující na bezdrátové uživatele

Odposloucháváním provozu mohou útočníci rozpoznat přítomnost klientů. Pokud klient (například osobní laptop na veřejném místě) není dostatečně zabezpečen, lze jej oklamat přítomností falešným přístupovým bodem se silnějším signálem k přilákáním na tento přístupový bod. Tímto může realizovat útok man-in-the middle a další útoky.

Zde Honeypot simuluje bezdrátového klienta, který je připojen k přístupovému bodu. Lze využít i více simulovaných klientů, například jeden pro každý protokol (ARP, TCP, UDP aj.) [3]



Obrázek 3.4: útok na bezdrátový přístupový bod

3.4 Nástroje Honeypot

3.4.1 KeyFocus – KFSensor

Úkolem každého Honeypotu je přitahovat a nalákat útočníky tak, že simuluje ohrožené systémové služby a ani *KFSenzor* není výjimkou.

Tím, že slouží, jako návnada je možné přesměrovat útoky z kritických systémů a zajistit vyšší úroveň bezpečí, než může být dosaženo pomocí firewallů a NIDS[5].

KFSensor je určen pro použití na operačním systému Windows v podnikovém prostředí a obsahuje mnoho funkcí, jako je dálkové řízení a emulace síťových protokolů systému Windows.

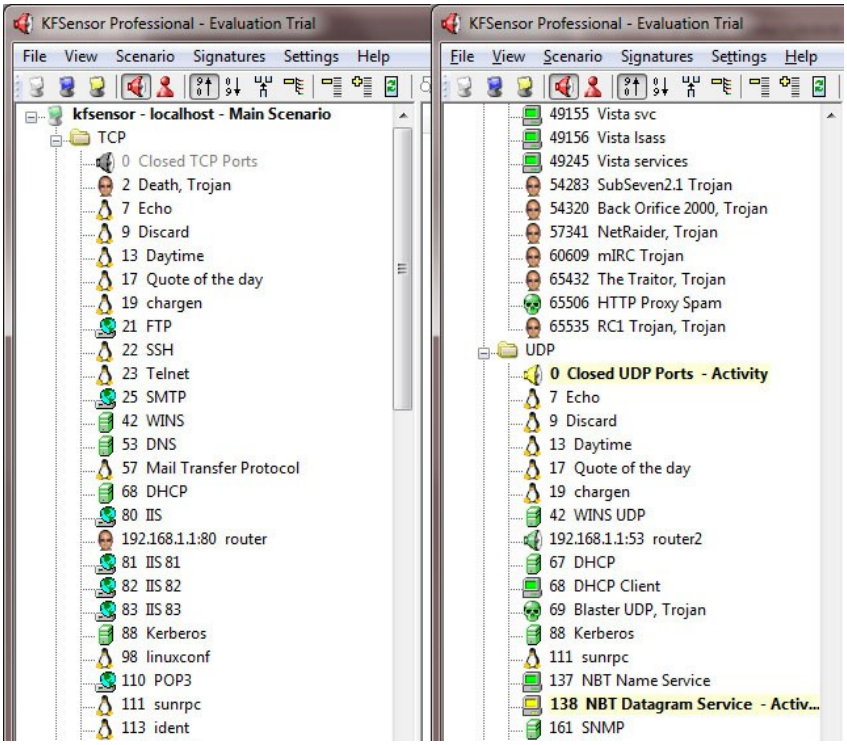
Na rozdíl od linuxových Honeypotů, jako je například *Honeyd* má *KFSensor* GUI[6] management, který dopomáhá ke snadné konfiguraci. Možnou nevýhodou je, že se jedná o komerční program, jehož základní cena začíná na 199 dolarech. Je možnost zakoupit i verzi Profesionál a Enterprise. [9]

3.4.1.1 ***Funkce:***

Monitorování všech portů

KFSensor monitoruje útoky na všech TCP a UDP portech, stejně jako detekci ICMP zpráv. Také monitoruje veškerou aktivitu v síti serverových aplikací Windows.

[5] Systémy pro detekci průniku do sítě
[6] Grafické uživatelské prostředí



Obrázek 3.5: Simulace služeb KFSensor

Vzdálená správa

KFSensor obsahuje schopnost řídit a monitorovat několik Honeypot zařízení zároveň. Pomocí senzorů získávat informace z různých částí sítě. Tyto sensory jsou monitorovány v reálném čase, což umožňuje okamžitý přehled útoků a jak k nim dochází.

K autentizaci využívá privátní a veřejný RSA[7] klíč o velikosti 3072 bitů a 256 bitové AES šifrování, pro zabezpečení komunikace mezi senzory.

IDS

KFSensor je první produkt, který kombinuje IDS a Honeypot systém. Jeho rychlý vyhledávač, má minimální dopad na výkon systému a dokáže zpracovávat tisíce pravidel.

3.4.1.2 Emulované služby

KFSensor nabízí celou řadu různých typů emulace. Ty mohou být rozšířená o využití vlastních skriptů. Zde je malý výběr podporovaných služeb:

Naslouchání portů

Nejzákladnější typ pasti je otevření portů. *KFSensor* přečte data, na něj poslána a záznamy událostí uloží do logovacího souboru.

[7] Šifrovací algoritmus 1983, Rivest, Shamir, Adleman

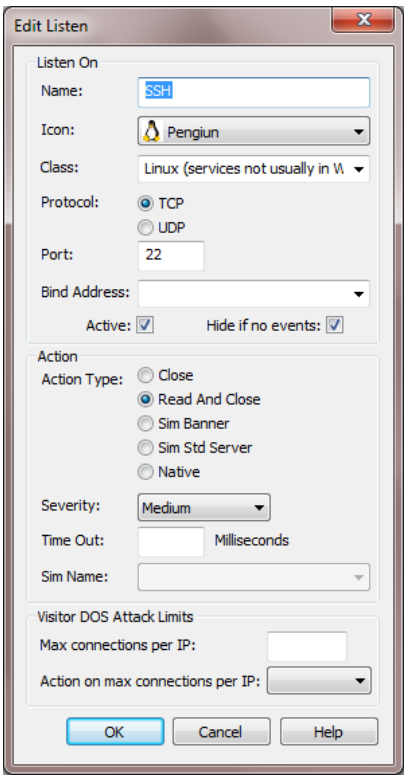
HTTP

Vytváří plně funkční webový server, který napodobuje *Microsoft IIS web server*. Server napodobuje řídící aspekty, jako je rozsah požadavků a kontrola vyrovnávací paměti na straně klienta.

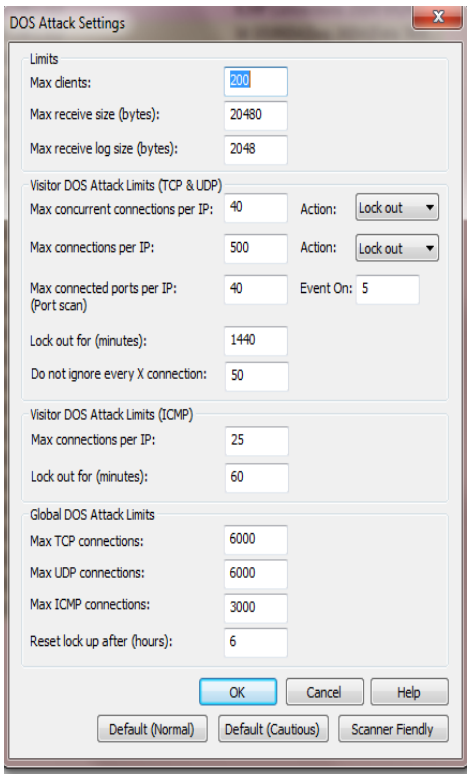
MySQL

Simulace, která zpracovává dotazy a dešifruje pakety do čitelné podoby. Umožňuje návštěvníkům přihlásit se a prohlížet schémata databáze.

Toto je jen stručný výběr emulovaných služeb. Mezi další patří například FTP, SSH, TELNET, LDAP aj.



Obrázek 3.6: Nastavení služby SSH



Obrázek 3.7: Nastavení ochrany proti DoS

Skripty

Své vlastní simulace je možné psát v jazyku *Perl* nebo *C*. *KFSensor* může využívat i skripty psané pro *Honeyd*.

DoS

Jeho další výhodou je ochrana proti Denial of Service (DoS). *KFSensor* obsahuje mechanismy proti DoS, které detekuji útok a přeruší spojení. [3][8]

[8] Celkový popis schopností naleznete na stránkách http://www.keyfocus.net/.

3.4.2 Honeyd

Honeyd je aplikace běžící v daemon režimu, který vytváří virtuální hostitele v síti. Hostitel může být nakonfigurován pro spuštění libovolné služby a může být upraven tak, aby simuloval spuštění na určitém operačním systému. *Honeyd* umožňuje pro jednotlivé hostitele žádat více adres, až 65536 pro simulaci LAN[9] sítě. *Honeyd* zlepšuje bezpečnost pomocí mechanismu IDS. Také odrazuje protivníky skrytím reálných systémů uprostřed virtuálních systémů. Dokonce je možné jednotlivé virtuální stroje otestovat pomocí nástroje ping, nebo použití traceroute.

Jakýkoliv druh služby na virtuálním stroji lze simulovat pomocí jednoduchého konfiguračního souboru nebo je možné připojení pomocí proxy na již běžící službu.

Podporuje vytvoření virtuální síťové topologie, včetně vyhrazených cest a tras. Na trasy lze aplikovat zpoždění a ztrátovost paketů, aby se topologie pro útočníky zdála reálnější. [10]

3.4.2.1 Funkce:

Honeyd podporuje funkce, které umožňují být velmi flexibilní při vytváření virtuálních hostitelů a sítí. Následující seznam podává stručný přehled různých funkcí, které *Honeyd* podporuje:

- Simuluje tisíce virtuálních počítačů ve stejný čas.
- Konfigurace libovolných služeb pomocí konfiguračního souboru:
  - Zahrnuje připojení proxy.
  - Pasivní snímání k identifikaci vzdálených počítačů.
- Simuluje operační systémy na úrovni TCP/IP protokolu:
  - Oklamání nástrojů *nmap* a *xprobe* (nástroje pro detekci OS).
  - Nastavitelný FIN-scan.
- Simulace libovolné topologie směrování:
  - Konfigurace zpoždění a ztrátovost paketů.
  - Asymetrické směrování.
  - Integrace fyzických strojů do topologie.
  - Distribuce *Honeyd* pomocí GRE tunelů.
- Subsystém virtualizace:
  - Spuštění skutečných UNIX služeb na virtuálním *Honeyd*: Web server, FTP server, atd.
  - Dynamické přidělování portů, iniciace síťových připojení na pozadí, atd.

Honeyd podporuje asymetrický trasy a její fyzické začleněných do virtuální síťové topologie. V důsledku toho je možné použít *Honeyd* jako jednoduchou síťovou simulaci. [10]

[9] Lokální síť, místní síť

3.4.3 Shrnutí

Mezi *KFSensor* a *Honeyd* existují patrné rozdíly. Pro *KFSensor* je výhodou přehledné grafické prostředí s jednoduchou konfigurací a již vytvořenými službami. *Honeyd* je náročný na konfiguraci, ale oproti *KFSensor* má velice důležitou funkci a to, že dokáže simulovat sítové prvky a přiřazovat jim IP adresy.

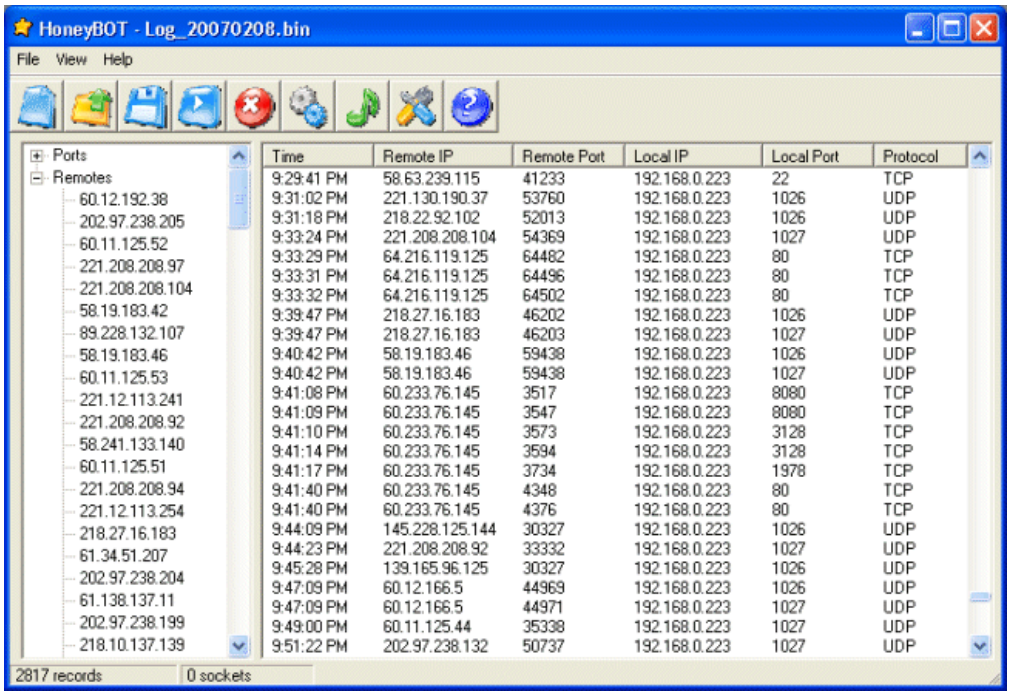
3.4.4 Ostatní

Existuje řada dalších nástrojů nebo projektů, ke tvorbě Honeypotů. U operačního systému Unix máme na výběr například *Honeypots, wifi_honeypot* aj. Tyto všechny nástroje vycházejí z projektu *Honeyd* a mají společné funkce i konfigurační soubory. Liší se jen obsahem skriptů a připojený nástrojů, které lze dodatečně doinstalovat i k původnímu *Honeyd*.

Na operačním systému Windows je již více různých možností Honeypotů. Zde uvedu *Honeyd-win*. Jedná se předělání Unix *Honeyd* na operační systém Windows.

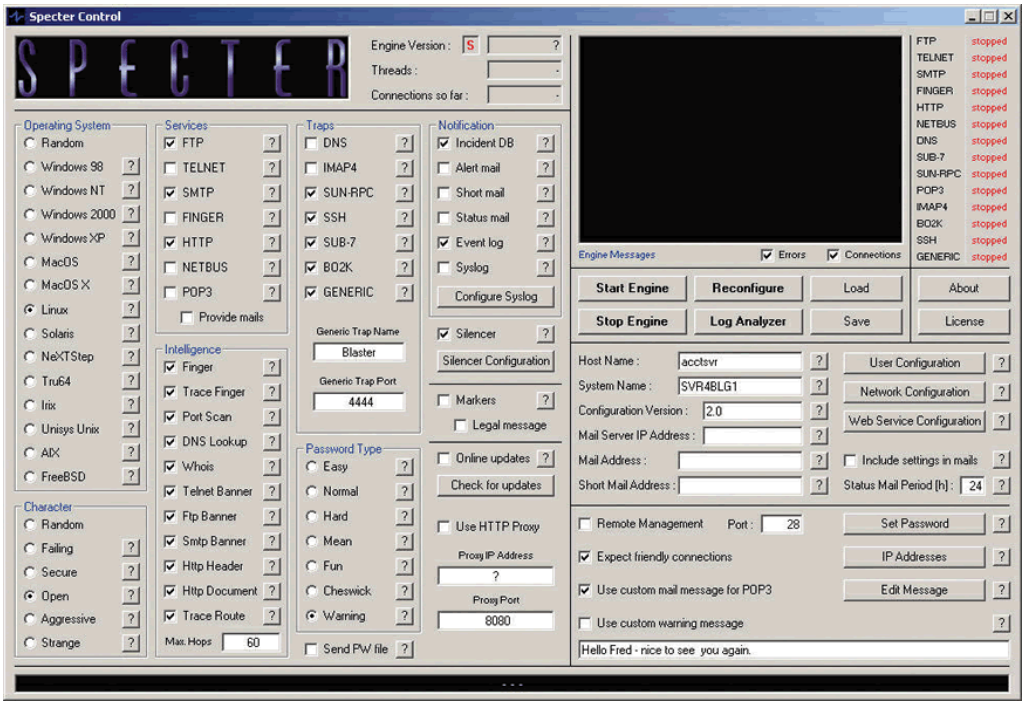
Honeybot

Jedná se o placenou verzi, kterou lze vyzkoušet na 30 dní. Oproti *KFSensor* nemá propracované uživatelské rozhraní a nepodporuje podrobnější konfiguraci.



Obrázek 3.8: HoneyBOT

Mezi další *Honeypot* s podporou IDS patří *SPECTER*. Bohužel ho nebylo možné vyzkoušet, protože nelze stáhnou ani jeho zkušební verzi. Hlavní nevýhodou většiny *Honeypot* založených na systému Windows je pořizovací cena, která se může vyšplhat až na několik tisíc korun.



Obrázek 3.9: Specter

4 Praktická implementace Wi-Fi Honeypot

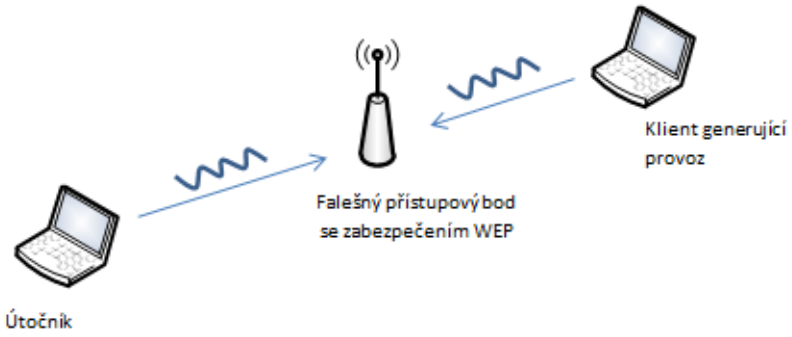
V této části bude předvedena instalace a zprovoznění požadovaných programů pro tvorbu Honeypotu.

4.1 Operační systém

Projekt je vytvořen na operačním systému Linux a to distribuce *BackTrack 5 R2*[10]. Jedná se o nadstavbu distribuce Ubuntu, zcela volně šiřitelná. Tato verze je speciálně přizpůsobená pro penetrační testy a monitorování sítě.

4.2 Topologie

Honeypot tvoří virtuální bezdrátový bod, který je zabezpečený protokolem WEP. Na bezdrátovou síť je připojen jeden klient, který generuje minimálního provoz. O zachytávání sítě se stará nástroj *airodump-ng* a provoz ukládá do souborů *cap*. Tyto soubory následně slouží k detekci případných útoků na náš přístupový bod. Pro vytváření log souborů je využit nástroj *Honeyd*.



Obrázek 4.1: Topologie použitého Honeypot

[10] http://www.backtrack-linux.org/

4.3 Nástroje pro vytvoření virtuální bezdrátové sítě

4.3.1 *dhcp3-server*

Pro připojení uživatelů na náš virtuální bod je potřeba vytvořit DHCP server. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, bránu a adresu DNS serveru.

DHCP server je nutné nainstalovat, aby ho bylo možné využívat.

```
#apt-get isntall dhcp3-server
```

Dále je nutné upravit konfigurační soubor */etc/dhcp3/dhcpd.conf*

```
ddns-update-style ad-hoc;
 default-lease-time 600;
 max-lease-time 7200;
 subnet 192.168.3.0 netmask 255.255.255.0 {
 option subnet-mask 255.255.255.0;
 option broadcast-address 192.168.3.255;
 option routers 192.168.3.19;
 option domain-name-servers 4.2.2.2;
 range 192.168.3.100 192.168.3.140;
 }
```

Tímto připojený klient dostane adresu v rozsahu 192.168.3.100-140.

4.3.2 *airmon-ng*[11]

Pomocí tohoto nástroje se spouští monitorovací mód na našem bezdrátovém rozhraní. To znamená, že umožňuje počítači s Wi-Fi kartou monitorovat síťový provoz v dosahu. Program je součásti balíku *aircrack-ng*.

Použití:

```
#airmon-ng <start|stop> <rozhraní> [kanál]
```

V našem případě použijeme příkaz #*airmon-ng,* ke zjištění bezdrátového rozhraní.

[11] Http://www.aircrack-ng.org/doku.php?id=airodump-ng [2012-05-03].

```
root@bt:~# airmon-ng

Interface       Chipset         Driver

wlan1           Ralink RT2870/3070      rt2800usb - [phy1]
wlan0           Atheros AR2425  ath5k - [phy0]
```

Obrázek 4.2: Výpis bezdrátového rozhraní

Zde vidíme dvě bezdrátové rozhraní *wlan1* a *wlan0.*

Příkazem *#airmon-ng start wlan1* zapneme monitorovací mód na námi zvoleném rozhraní.

```
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
1289    wpa_supplicant
1296    dhcpcd-bin
1298    dhcpcd-bin
Process with PID 1289 (wpa_supplicant) is running on interface wlan0
Process with PID 1298 (dhcpcd-bin) is running on interface wlan0


Interface       Chipset         Driver

wlan1           Ralink RT2870/3070      rt2800usb - [phy1]
                                (monitor mode enabled on mon0)
wlan0           Atheros AR2425  ath5k - [phy0]
```

Obrázek 4.3: Monitorovací mód

Na obrázku 4.3 můžeme vidět zapnutí monitorovacího módu na rozhraní *wlan0*.

4.4 *airbase-ng*[12]

Airbase-ng je víceúčelový nástroj, jehož cílem je útok na klienty. Hlavní úkolem je realizace falešného přístupového bodu, spojení klientů na tento bod a zabránit jim připojení na skutečný.

Vytvoří virtuální rozhraní *at(*x), které může přijímat dešifrované pakety nebo odesílat šifrované pakety.

Upozornění: *Airbase-ng* může narušit správnou funkci přístupového bodu na stejném kanálu.

Použití:

```
#airbase-ng <volba> <rozhraní>
```

[12] http://www.aircrack-ng.org/doku.php?id=airbase-ng [2012-05-03].

Syntaxe, kterou použijeme:

```
#airbase-ng -e Pekarska -c 9 mon0 -w 1234567890 -W 1 -a F81:11:16:9C:7C
```

Nejčastější volbou je "-e" pro označení přístupového bodu, toto je pouze jedno z mnoha možností. Mezi další často používané patří:

```
-a bssid: nastavení MAC adresy
-w WEP key: nastavení WEP klíče
-W 0|1: [don't] set WEP flag in beacons 0|1 (default: auto)
-c channel : nastavení kanálu, na kterém běží přístupový bod
-X: skrýt ESSID (--hidden)
-z type: nastavení  WPA1 tags. 1=WEP40 2=TKIP 3=WRAP 4=CCMP 5=WEP104
-Z type: stejné jako -z, ale pro WPA2
```

```
root@bt:~# airbase-ng -e "Pekarska" -c 9 mon0 -w 1234567890 -W 1 -a F8:D1:11:16:
9C:7C
15:42:58  Created tap interface at0
15:42:58  Trying to set MTU on at0 to 1500
15:42:58  Trying to set MTU on mon0 to 1800
15:42:59  Access Point with BSSID F8:D1:11:16:9C:7C started.

15:43:31  Client A8:26:D9:D1:4E:09 associated (WEP) to ESSID: "Pekarska"
15:43:31  Client A8:26:D9:D1:4E:09 associated (WEP) to ESSID: "Pekarska"
```

Obrázek 4.4: WEP

Na obrázku 4.4 vidíme spuštění přístupového bodu se zabezpečením WEP.

Obrázek 4.5: Zobrazení falešného AP

Na obrázku 4.6 lze vidět vytvoření přístupového bodu na rozhraní at0 s MAC adresou F8:D1:11:16:9C:7C.

Aby DHCP server mohl přiřadit adresy, musí se přiřadit našemu rozhraní *at0* IP, masku a GW.

```
ifconfig at0 up
ifconfig at0 192.168.3.1 netmask 255.255.255.0
route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.3.1
```

```
root@bt:~# ifconfig
at0       Link encap:Ethernet  HWaddr f8:d1:11:16:9c:7c
          inet addr:192.168.3.1  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::fad1:11ff:fe16:9c7c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:468 (468.0 B)
```

Obrázek 4.6: Výpis virtuálního rozhraní

4.5 *Airdump-ng*[13]

Airodump-ng se používá pro zachycení paketů 802.11 rámců a je vhodný zejména pro sběr WEP inicializačních vektorů (IV). Pokud máte GPS přijímač připojený k počítači, *airodump-ng* je schopen zaznamenávat souřadnice z nalezených přístupových bodů. Získané informace zapisuje do několika souborů, které obsahují údaje o přístupových bodech a klientech.

Použití:

```
#airodump-ng <volba> <rozhraní>
```

Naše syntaxe:

```
#airodump-ng -w cap --bssid F8:D1:11:16:9C:7C --channel 9 mon0
-w: zápis do souboru
-- channel: monitorovaný kanál
-- bssid: monitoravná MAC adresa
```

Více informací a voleb najdete v manuálu *#airodump-ng –help*

[13] http://www.aircrack-ng.org/doku.php?id=airodump-ng [2012-05-03].

```
CH  9 ][ Elapsed: 2 mins ][ 2012-04-27 16:29

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:D1:11:16:9C:7C    0 100     2572        3    0   9  54   WEP  WEP    OPN  Pekarska

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

F8:D1:11:16:9C:7C  A8:26:D9:D1:4E:09  -42    0 - 1      0      104
```

Obrázek 4.7: Záznam síťového provozu

4.6 *Honeyd*

Jak už bylo napsáno v kapitole 3 *Honeyd* je aplikace běžící na pozadí a monitorující síť.

Honeyd je součástí OS Backtrack, tak ho není potřeba instalovat, popřípadě se nainstaluje jednoduchým příkazem `apt-get install honeyd`.

4.6.1 Spuštění *Honeyd*

Základní příkaz na spuštění:

```
#honeyd <volby>
```

Základní popis operátorů:

```
-d: umožnuje spuštění debugmod s výpisem událostí na obrazovku
-l (logfile): místo kde se budou ukládat záznamy o síti
-f: umístění konfiguračního souboru (honeyd.conf)
-i: rozhraní, na kterém honeyd poslouchá
```

4.6.2 Konfigurace

O běh programu se stará konfigurační soubor, který si můžeme pojmenovat jakýmkoliv způsobem. K určení konfiguračního souboru nám slouží parametr `-f` (file), tedy `-f <cesta>`.

Ukázka jednoduché konfigurace:

```
create windowsxp
 set windows personality "Microsoft Windows XP Professional"
 add windowsxp tcp port 135 open
 add windowsxp tcp port 139 open
 add windowsxp tcp port 137 open
 add windowsxp udp port 137 open
 add windowsxp udp port 138 open
 set windowsxp default tcp action block
 set windowsxp default udp action block
 bind 192.168.3.2 windowsxp
```

Tímto nastavením jsme si vytvořili virtuální počítač s názvem *windowsxp*.

Popis a význam jednotlivých příkazů:

```
 create windowsxp
```

Vytvoření stroje s názvem *windowsxp*. Tento popis slouží pouze k identifikaci v rámci *honeyd* a není nikde zobrazen.

```
 set windows personality "Microsoft Windows XP Professional"
```

Nastavení otisku (fingerprint), který bude *honeyd* na žádost útočníků posílat. Přesný název otisku je napsán v souboru *nmap.assoc*.

Ukázka souboru *nmap.assoc*.

```
Microsoft Windows Millennium Edition (Me);Microsoft Windows XP Professional
Microsoft Windows 2000 SP3;Microsoft Windows 2000/2000SP1/2000SP2/2000SP3
Microsoft Windows 2000 SP3;Microsoft Windows 2000/2000SP1/2000SP2/2000SP3
Microsoft Windows 2000 Professional SP2 or Windows XP SP1;Microsoft Windows XP
Professional
```

```
add windowsxp udp port 138 open
```

Otevření UDP portu 138.

```
set windowsxp default UDP action block
```

Nastavení chování při skenování portů. *Honeyd* bude ostatní porty hlásit jako uzavřené.

```
bind 10.0.0.2 windowsxp
```

Přiděleni IP adresy k virtuálnímu stroji.

Pro vytvoření služeb či simulaci serveru se používají skript soubory. Tyto soubory se vytvoří při instalaci nebo je lze stáhnout *http://www.honeyd.org/contrib.php*.

```
add ftpserver tcp port 21 "sh ftp.sh"
```

Při připojení na port 21, bude skript reagovat na příkazy.

```
add mailserver tcp port 25 "sh smtp.sh"
add mailserver tcp port 110 "sh pop3.sh"
```

V našem případě nemusíme simulovat jakoukoliv službu, tak nám postačí použít *Honeyd* jen na logování.

```
#honeyd -d -l /root/Desktop/honey/logwep.txt -i at0
```

Ukázka výpisu z log souboru:

```
2012-05-02-20:01:52.1798 udp(17)- 192.168.3.130 63931 224.0.0.252 5355: 52
2012-05-02-20:01:52.1923 udp(17) - 192.168.3.130 137 192.168.3.255 137: 78
2012-05-02-20:01:52.1978 udp(17) - 192.168.3.130 137 192.168.3.255 137: 78
2012-05-02-20:01:52.2042 udp(17) - 192.168.3.130 137 192.168.3.255 137: 78
2012-05-02-20:01:52.2105 udp(17) - 192.168.3.130 137 192.168.3.255 137: 78
2012-05-02-20:01:52.2185 udp(17) - 192.168.3.130 137 192.168.3.255 137: 78
```

Význam polí:

1) datum
2) protokol
3) zdrojová ip, port, cílová ip, port
4) poslední pole obsahuje proměnné informace (fingerprint, velikost paketu atd.)

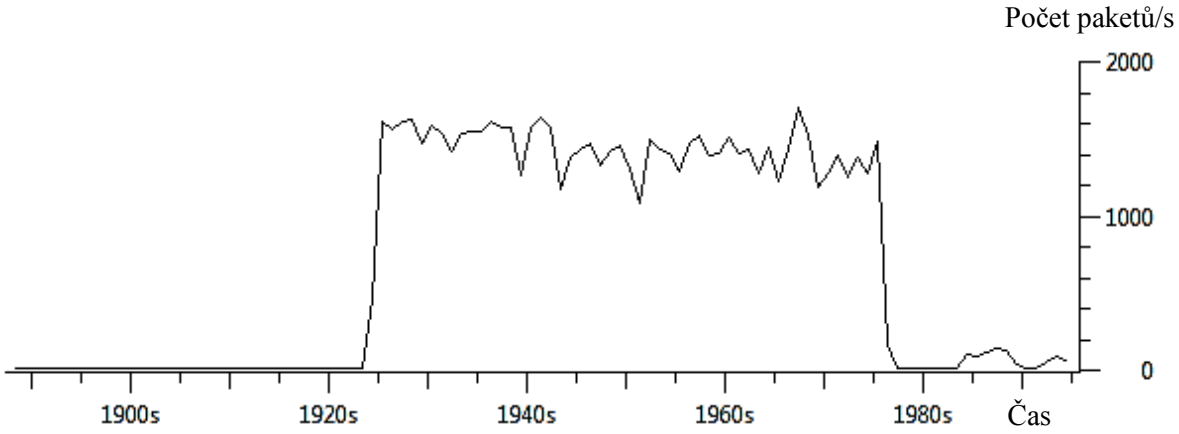
5 Statistika útoků

5.1 Statistika testovaného prostředí

V testovaném prostředí se nezachytával reálný provoz sítě. Vytvářely se referenční body, které později sloužily k porovnávání a detekování útoků na přístupový bod. Jak již bylo zmíněno v kapitole 4, byl vytvořen virtuální přístupový bod se zabezpečením WEP. Na kterém se testovaly útoky. Záznamy jsou uložené ve formátu *cap*. K analýze byl použit program Wireshark[14].

5.2 Typy útoku

Před samotnou analýzou je vhodné se podívat na graf vytížení sítě, který nám usnadní práci a nebudeme bezcílně procházet bezpočtem paketů.



Obrázek 5.1: Graf provozu

Pomocí filtrů provozu lze záznam a grafy upravit, aby zobrazovaly námi požadované informace.

```
wlan.sa == 00:24:2b:c1:b7:ae
```

Tento filtr nám zobrazí pouze provoz na wlan zdrojové MAC adrese 00:24:2b:c1:b7:ae

[14] Program pro analýzu a monitorování provozu v počítačových sítích

5.2.1 Deauthentication

Tento útok může sloužit k odpojení uživatele od sítě. Jakmile se opět připojí, útočník získá informace o SSID, i když je skryté a zaznamená inicializační vektory. U zabezpečení WPA je tento útok důležitý pro zachycení „handshake“ a následné zjištění hesla.

```
1906 10:54:17.892432 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2545, FN=0, Flags=........
1907 10:54:17.896528 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2546, FN=0, Flags=........
1908 10:54:17.900624 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2548, FN=0, Flags=........
1909 10:54:17.902672 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2549, FN=0, Flags=........
1910 10:54:17.910354 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2552, FN=0, Flags=........
1911 10:54:17.916498 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2555, FN=0, Flags=........
1912 10:54:17.922642 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2557, FN=0, Flags=........
1913 10:54:17.924178 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2558, FN=0, Flags=........
1914 10:54:17.928786 Tp-LinkT_16:9c:7c  Broadcast  802.11 26 Deauthentication, SN=2559, FN=0, Flags=........
```

Obrázek 5.2: Deautentizace

```
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: Tp-LinkT_16:9c:7c (f8:d1:11:16:9c:7c)
BSS Id: Tp-LinkT_16:9c:7c (f8:d1:11:16:9c:7c)
```

Obrázek 5.3: Deautentizace

Toto je již první náznak příchozího útoku.

5.2.2 Injekce paketů

Nejčastějším způsobem generování dat je injekce ARP paketů. Útočník provádí „*deautentizační*“ útok na připojeného klienta. Když se klient snaží připojit, vyšle ARP paket. Přístupový bod je nucen odpovědět. V každé odpovědi se nachází IV, který útočník potřebuje k dešifrování hesla. Po zachycení dostatečného množství dokáže dešifrovat klíč.

```
4400 11:09:20.24681 Tp-LinkT_16:05:25 Broadcast                ARP 68 Who has 192.168.3.130?  Tell 0.0.0.0
4401 11:09:20.24681 Tp-LinkT_16:05:25 Broadcast                ARP 68 Who has 192.168.3.1?  Tell 192.168.3.130
4402 11:09:20.24684 Tp-LinkT_16:05:25 Broadcast                ARP 68 Who has 192.168.3.130?  Tell 0.0.0.0
4403 11:09:20.24736 Tp-LinkT_16:05:25 Broadcast                ARP 68 Who has 192.168.3.1?  Tell 192.168.3.130
4404 11:09:20.24736 Tp-LinkT_16:9c:7c HonHaiPr_c1:b7:ae        ARP 68 192.168.3.1 is at f8:d1:11:16:9c:7c
4405 11:09:20.24732 Tp-LinkT_16:05:25 Broadcast                ARP 68 Who has 192.168.3.1?  Tell 192.168.3.130
4406 11:09:20.24736 Tp-LinkT_16:05:25 Broadcast                ARP 68 Who has 192.168.3.1?  Tell 192.168.3.130
4407 11:09:20.24736 Tp-LinkT_16:9c:7c HonHaiPr_c1:b7:ae        ARP 68 192.168.3.1 is at f8:d1:11:16:9c:7c
```

Obrázek 5.4: Injekce ARP

5.2.3 Authentication, Association Flood

Tento útok má za úkol vyřadit z provozu přístupový bod. Útočník posílá Authentication a Association pakety na cílový bod. Přístupový bod zachytí veškeré žádosti a snaží se na ně odpovědět. Jelikož má omezenou kapacitu paměti, dospěje do bodu, kdy nebude schopen obsluhovat více příkazů a to vede až ke shození přístupového bodu.

```
225856 Tp-LinkT_16:9c:7c  Cisco_96:ae:da     802.11 52 Association Response, SN=0, FN=0, Flags=........, SSID=Broadcast
225856 Tp-LinkT_16:9c:7c  Cisco_96:ae:da     802.11 52 Association Response, SN=0, FN=0, Flags=........, SSID=Broadcast
227904 Tp-LinkT_16:9c:7c  Cisco_96:ae:da     802.11 52 Association Response, SN=0, FN=0, Flags=........, SSID=Broadcast
227904 Tp-LinkT_16:9c:7c  BelkinCo_bd:ec:1a  802.11 52 Association Response, SN=0, FN=0, Flags=........, SSID=Broadcast
227904 Tp-LinkT_16:9c:7c  BelkinCo_bd:ec:1a  802.11 52 Association Response, SN=0, FN=0, Flags=........, SSID=Broadcast
234002 Hewlett-_cb:8f:20  Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Hewlett-_cb:8f:20  Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Hewlett-_cb:8f:20  Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Hewlett-_cb:8f:20  Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Hewlett-_cb:8f:20  Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Hewlett-_cb:8f:20  Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Hewlett-_cb:8f:20  Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Agere_2d:4c:f2     Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Agere_2d:4c:f2     Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234516 Agere_2d:4c:f2     Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
234514 Agere_2d:4c:f2     Tp-LinkT_16:9c:7c  802.11 54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
```

Obrázek 5.5: Authentication, Association Flood

Tento druh útoků patří do skupiny DoS útoku. Pakety přicházejí z různých falešných adres, proto je nemožné zjistit pravou adresu útočníka. Tento typ útoků je velmi lehce zjistitelný a velmi náročný na ochranu.

5.2.4 Beacon Flood

Tento druh útoku není přímo mířený na přístupový bod, ale dokáže zahltit blízké okolí falešnými „beacon frame“, které znemožňují uživatelovi zjistit přístupové body v okolí.

```
826 24:43:70:0f:49:95  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
975 51:4d:de:ec:c3:68  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
173 3b:b7:f5:01:24:8c  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
661 7b:b5:16:13:60:86  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
020 6d:e4:5f:4c:d1:22  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
596 Tp-LinkT_16:9c:7c  Broadcast  802.11    77 Beacon frame, SN=1455, FN=0, Flags=........, BI=100, SSID=Pekarska
237 b4:0c:d9:a9:0d:fd  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
443 35:b1:38:7e:94:31  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
774 9d:8b:ca:66:63:5e  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
016 78:d0:42:d7:1c:13  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
409 f9:d1:20:d2:7a:2d  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
472 d0:b0:de:08:2e:73  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
680 Tp-LinkT_16:9c:7c  Broadcast  802.11    77 Beacon frame, SN=1456, FN=0, Flags=........, BI=100, SSID=Pekarska
864 Tp-LinkT_16:9c:7c  Broadcast  802.11    85 Beacon frame, SN=1455, FN=0, Flags=........, BI=100, SSID=Pekarska[M
927 Tp-LinkT_16:9c:7c  Broadcast  802.11    85 Beacon frame, SN=1456, FN=0, Flags=........, BI=100, SSID=Pekarska[M
091 66:e4:31:31:4a:94  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
187 e5:94:52:05:66:cd  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
420 32:36:7d:11:3e:ab  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
595 84:78:da:07:98:20  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
833 ad:fe:04:df:2f:4f  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
444 79:ac:dd:f6:bd:1c  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
898 Tp-LinkT_16:9c:7c  Broadcast  802.11    77 Beacon frame, SN=1457, FN=0, Flags=........, BI=100, SSID=Pekarska
700 a1:41:94:7b:48:2c  Broadcast  802.11   117 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Pekarska
```

Obrázek 5.6: Beacon Flood

5.3 Statistika reálného prostředí

Samotná reálná statistika probíhala v období jednoho měsíce, po který se sledoval provoz na vytvořených přístupových bodech. Celkem byly vytvořeny 3 místa, kde probíhalo monitorování sítě a to vesnice Malé Heraltice, městské sídliště Opava-Kateřinky a prostory školy Slezské univerzity v Opavě. Pomocí referenčních bodů lze pak určit případné útoky a přístupy na tyto přístupové body.

5.3.1 Malé Heraltice

Tato vesnice se nachází přibližně 20 km od Opavy a trvalých obyvatel zde žije okolo 300. Virtuální bod byl vytvořen přibližně 50m od vysílače místního poskytovatele bezdrátové sítě.

Podle předpokladu, zachycený provoz na náš *Honeypot* byl téměř nulový a nepodařilo se zachytit žádný útok, krom testovaných útoků.

5.3.2 Opava-Kateřinky

Jedná se o hustě obydlenou oblast v Opavě, kde může bydlet přibližně okolo 1000 obyvatel. V této lokalitě proběhlo monitorování již s výsledkem a dokázalo zachytit provoz na námi vytvořené síti.

Jednalo se převážně o pokusy připojení k naší síti. Těchto pokusu bylo pouhých sedm. Ze záznamu šlo vyčíst, že se nedostali dále než k zadávání hesla. Z toho třikrát z jedné MAC adresy

```
BSS Id: Tp-LinkT 16:9c:7c (f8:d1:11:16:9c:7c)
Source address: Azurewav_2b:64:be (00:15:af:2b:64:be)
Destination address: Tp-LinkT_16:9c:7c (f8:d1:11:16:9c:7c)
```

Obrázek 5.7: MAC adresa

Na obrázku 5.7 je zobrazena MAC adresa uživatele, který se snažil třikrát připojit k síti.

```
51354 11:54:51.144924 Htc_d1:4e:09      Tp-LinkT_16:9c:7c  EAPOL      37 Start
51355 11:54:51.144926 Htc_d1:4e:09      Tp-LinkT_16:9c:7c  EAPOL      37 Start
51362 11:54:51.151068 Htc_d1:4e:09      Tp-LinkT_16:9c:7c  EAPOL      37 Start
51364 11:54:51.151070 Htc_d1:4e:09      Tp-LinkT_16:9c:7c  EAPOL      37 Start
51366 11:54:51.151068 Htc_d1:4e:09      Tp-LinkT_16:9c:7c  EAPOL      37 Start
```

Obrázek 5.8: Zahájení připojení

Při monitorování v této lokalitě jsem zaznamenal celkem 20 sítí. Potěšující je, že většina těchto sítí používá minimálně WPA zabezpečení. Jen je chyba, že hodně sítí využívá stejného kanálů. Toto může vést ke vzájemnému rušení a ke kolizím v síti.

Tabulka 1: Seznam přístupových bodů, Kateřinky

ESSID	*BSSID*	*CH*	*Encryption*
00:0B:6B:83:F6:99	*BiBi-Game*	*3*	*OPN*
00:0B:6B:2B:C4:90	*SARAINET-CZECHWOOD*	*13*	*OPN*
00:23:CD:D8:4B:A4	*Horinku*	*8*	*OPN*
00:21:63:9C:16:7B	*VOIP*	*1*	*WEP*
00:0C:42:68:73:68	*East_AirNet*	*7*	*WEP*
00:23:CD:D9:AC:2A	*salvova*	*6*	*WEP*
00:27:19:E8:FE:52	*Santos*	*8*	*WPA*
38:72:C0:09:9B:46	*Internet*	*7*	*WPA*
00:21:63:9C:16:7A	*Ahoj*	*1*	*WPA*
38:72:C0:96:73:BC	*Karcher*	*2*	*WPA*
00:19:5B:B4:70:55	*Gabi-net*	*6*	*WPA*
00:1F:1F:04:EA:05	*AP*	*1*	*WPA*
90:E6:BA:43:65:95	*q-159qaywsx*	*12*	*WPA2*
94:44:52:56:3F:72	*Belkin_G_Wireless_563F72*	*6*	*WPA2*
00:22:B0:B4:AD:1C	*dlink*	*1*	*WPA2*
00:22:75:F1:84:A7	*Branomrdek*	*6*	*WPA2*
94:0C:6D:A4:8C:26	*Mates*	*6*	*WPA2*
74:EA:3A:D7:BC:8A	*GOstudio*	*1*	*WPA2*
F4:EC:38:FE:75:A2	*CZNetFreeKasparkovi*	*1*	*WPA2*
F4:EC:38:9B:36:D0	*Maxnet_Kain*	*3*	*WPA2*

5.3.3 Slezská univerzita

Tento bod byl umístěn v jedné z učeben Slezské univerzity. Zde bylo hlavní místo, kde byl zprovozněn Honeypot. Z důvodů velkého pohybu studentů, a že se jedná o veřejnou budovu, byla zde velká šance na zaznamenání útoků. Toto tušení se taky potvrdilo a úspěšně byl proveden záznam o útoku na naší síť.

Jednalo se přímo o útok na prolomení naší sítě. Útok započal v pátek 20. Dubna v 18:55:06.

```
Arrival Time: April 21, 2012 18:55:09.223256000 Střední Evropa (letní čas)
```

V první části byl spuštěn deauthentication útok, který byl spuštěn přímo na klienta. Celkem bylo posláno 949 paketů na odpojení uživatele od sítě. Pomocí filtru `frame.len == 26 && wlan.sa == 00:25:22:05:d6:5a` se nám zobrazí námi požadovaný proces.

```
Destination address: Tp-LinkT_16:9c:7c (f8:d1:11:16:9c:7c)
Source address: AsrockIn_05:d6:5a (00:25:22:05:d6:5a)
BSS Id: Tp-LinkT_16:9c:7c (f8:d1:11:16:9c:7c)
```

Obrázek 5.9: Zdroj útoku

Z obrázku 5.9 jsme se dozvěděli, že útok pocházel z adresy `00:25:22:05:d6:5a` a směřoval na náš přístupový bod. Bohužel se nemůžeme dozvědět, zda to byla skutečná adresa, nebo si ji onen útočník změnil.

Jakmile se náš klient odpojil a znovu připojil, rozběhla se tzv. injekce paketů. Kdy útočník začal generovat provoz dvěma způsoby. Prvním způsobem bylo generování ARP dotazů, kdy přístupový bod je nucen odpovědět na ARP žádosti a v každé odpovědi generuje IV. Těchto žádostí vygeneroval útočník okolo 10 000.

```
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
AsrockIn_05:d6:5a       Broadcast           ARP          68 Who has 192.168.3.130?  Tell 0.0.0.0
```

Obrázek 5.10: ARP injekce

K injekci ARP paketu byl přidán útok, který má za úkol vybrat specifický paket a ten je následně automaticky opakován, aby generoval další provoz. Jedná se tzv, „*natural packet replay*“.

U nás využil protokolu NBNS.

192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>
192.168.3.130	192.168.3.255	NBNS	100 Name query NB ISATAP<00>

Obrázek 5.11: NBNS injekce

Díky dostatečnému provozu sítě díky ARP a NBNS injekci lze odvodit, že útočník zachytil dostatečný počet IV k dešifrování WEP.

To se vzápětí potvrdilo, kdy se objevil požadavek na DHCP server (*DHCP Request)* z adresy útočníka.

```
0.0.0.0 255.255.255.255DHCP     370    DHCP Request-Transaction
```

```
⊟ Option: (t=53,l=1) DHCP Message Type = DHCP Request
    Option: (53) DHCP Message Type
    Length: 1
    Value: 03
⊟ Option: (t=61,l=7) Client identifier
    Option: (61) Client identifier
    Length: 7
    Value: 0100242bc1b7ae
    Hardware type: Ethernet
    Client MAC address: AsrockIn_05:d6:5a (00:25:22:05:d6:5a)
```

Obrázek 5.12: Požadavek na DHCP

Druhý zaznamenaný útok, byl proveden v úterý 10. Dubna Jednalo o útok typu DoS. Později během týdne jsem se dozvěděl, že se jednalo o zkušební útok v rámci výuky na univerzitě.

Útok byl proveden metodou Authentication, Association Flood. Tento útok vede ke shození přestupového bodu zahlcením vyrovnávací paměti. Jelikož přístupový bod běžel simulován přes počítač, nepodařilo se ho pomocí tohoto útoku shodit. Kdy využívá výkonného hardware od počítače.

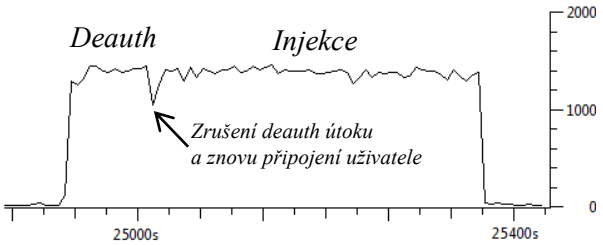
```
SmcNetwo_e2:b5:ca       Tp-LinkT_16:9c:7c   802.11       54 Association Request, SN=0, FN=0, Flags=........, SSID=Pekarska
ProximWi_4d:3d:34       Tp-LinkT_16:9c:7c   802.11       30 Authentication, SN=0, FN=0, Flags=........
ProximWi_4d:3d:34       Tp-LinkT_16:9c:7c   802.11       30 Authentication, SN=0, FN=0, Flags=........
ProximWi_4d:3d:34       Tp-LinkT_16:9c:7c   802.11       30 Authentication, SN=0, FN=0, Flags=........
Tp-LinkT_16:9c:7c       SmcNetwo_e2:b5:ca   802.11       46 Association Response, SN=0, FN=0, Flags=........
Tp-LinkT_16:9c:7c       SmcNetwo_e2:b5:ca   802.11       46 Association Response, SN=0, FN=0, Flags=........
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       30 Authentication, SN=0, FN=0, Flags=........
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       30 Authentication, SN=0, FN=0, Flags=........
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       30 Authentication, SN=0, FN=0, Flags=........
ProximWi_4d:3d:34       Tp-LinkT_16:9c:7c   802.11       30 Authentication, SN=0, FN=0, Flags=........
ProximWi_4d:3d:34       Tp-LinkT_16:9c:7c   802.11       30 Authentication, SN=0, FN=0, Flags=........
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       30 Authentication, SN=0, FN=0, Flags=........
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       30 Authentication, SN=0, FN=0, Flags=........
Tp-LinkT_16:9c:7c       SmcNetwo_e2:b5:ca   802.11       52 Association Response, SN=0, FN=0, Flags=........, SSID=Broadcast
Tp-LinkT_16:9c:7c       SmcNetwo_e2:b5:ca   802.11       52 Association Response, SN=0, FN=0, Flags=........, SSID=Broadcast
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       36 Authentication, SN=0, FN=0, Flags=........, SSID=Broadcast
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       36 Authentication, SN=0, FN=0, Flags=........, SSID=Broadcast
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       36 Authentication, SN=0, FN=0, Flags=........, SSID=Broadcast
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       36 Authentication, SN=0, FN=0, Flags=........, SSID=Broadcast
Tp-LinkT_16:9c:7c       ProximWi_4d:3d:34   802.11       36 Authentication, SN=0, FN=0, Flags=........, SSID=Broadcast
ProximWi_4d:3d:34       Tp-LinkT_16:9c:7c   802.11       30 Authentication, SN=0, FN=0, Flags=........
```

Obrázek 5.13: DoS útok

U tohoto útoku je nemožné zjistit, kdo za ním stojí, jelikož se náhodně generují zdrojové MAC adresy.

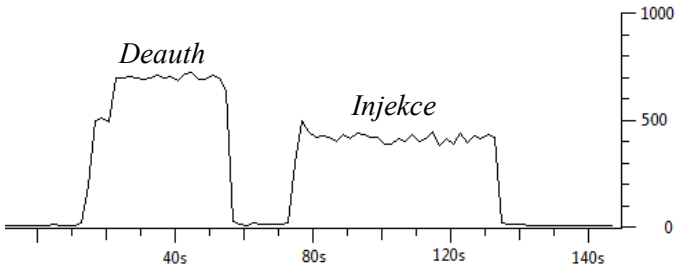
Porovnání útoků:

Hned prvním viditelným rozdílem mezi simulovaným a skutečným útokem byla charakteristika grafu. Na grafu z reálného provozu vidíme, že útoky probíhaly okamžitě po sobě.



Obrázek 5.14: Graf skutečného provozu

Oproti simulovaného provozu, kde jsou prodlevy mezi jdednotlivými útoky a taky, že útoky proběhly hned na začátku monitorování. Oproti realnému provozu, kde k tůtoku došlo přibližně po 7 hodinách.



Obrázek 5.15 Graf simulovaného provozu

Dalším rozdílem byl objem přenosu, kdy jsem při simulování nepotřeboval vygenerovat vysoký počet paketů pro shození sítě a následnou injekci.

Závěr:

Zda byl i první útok o prolomení WEP jen součásti výuky, nebo se jednalo o skutečný útok, jsem již nezjistil. Ze zachycených dat lze usoudit, že se útoky na bezdrátové sítě objevují jen zřídka. Zajímavé můžou být výsledky z mezinárodního letiště nebo velkého autobusového či vlakového nádraží.

Jako správce sítě bych v žádném případě nepoužil zabezpečení WEP, které bylo prolomeno do 10 minut. Jedinou zatím nejspolehlivější ochranou proti útokům na bezdrátové sítě je použití RADIUS serveru, kdy útočník nemá šanci odchytit provoz, který by vedl až dešifrování přístupových informací.

Dále přikládám seznam přístupových bodů v budově Slezské univerzity.

Tabulka 2: Seznam přístupových bodů, SLU

ESSID	*BSSID*	*CH*	*Encryption*
SUbn01	*00:4F:62:04:FD:0B*	*2*	*OPN*
su-fyzika-audio	*00:02:72:5D:2B:E5*	*11*	*OPN*
su-host	*00:17:DF:94:AC:32*	*6*	*OPN*
su-host	*00:17:DF:94:AA:C2*	*1*	*OPN*
Ufon1999	*94:0C:6D:A3:A2:DC*	*1*	*WEP*
FPF-SU-Dekan	*00:0D:54:A3:A9:17*	*9*	*WEP*
Chameleon	*38:72:C0:90:1C:15*	*3*	*WPA*
Hertel	*E8:39:DF:9A:4D:00*	*7*	*WPA*
su-zam	*E8:04:62:F7:A0:72*	*11*	*WPA2*
su-fyzika	*E8:04:62:F7:A0:70*	*11*	*WPA2*
su-fyzika	*00:17:DF:94:A7:51*	*1*	*WPA2*
su-fyzika	*E8:04:62:F7:99:41*	*1*	*WPA2*
su-zam	*68:BD:AB:84:4C:F2*	*6*	*WPA2*
su-fyzika	*68:BD:AB:84:4C:F0*	*6*	*WPA2*
su-fyzika	*00:17:DF:94:A3:01*	*11*	*WPA2*
su-fyzika	*00:17:DF:94:AC:31*	*6*	*WPA2*
su-fyzika	*00:17:DF:94:AA:C1*	*1*	*WPA2*
JARMILA	*D8:5D:4C:FB:A2:10*	*11*	*WPA2*
mojeWifi	*1C:AF:F7:8D:5E:BA*	*6*	*WPA2*
WiFi D-Link	*00:21:91:EC:A9:27*	*1*	*WPA2*
TP-LINK_EDB0E4	*00:27:19:ED:B0:E4*	*10*	*WPA2*
eduroam	*E8:04:62:F7:A0:71*	*11*	*WPA2*
eduroam	*00:17:DF:94:A7:50*	*1*	*WPA2*
eduroam	*E8:04:62:F7:99:40*	*1*	*WPA2*
eduroam	*68:BD:AB:84:4C:F1*	*6*	*WPA2*
eduroam	*00:17:DF:94:A3:00*	*11*	*WPA2*
eduroam	*00:17:DF:94:AC:30*	*6*	*WPA2*
eduroam	*00:17:DF:94:AA:C0*	*1*	*WPA2*

Z této tabulky lze vyčíst jednu závažnou bezpečnostní chybu a to použití WEP protokolu u přístupového bodu *FPF-SU-Dekan* .

6 Teoretický návrh pravidel a algoritmů pro omezení a eliminaci hrozeb

6.1 Základní pravidla zabezpečení bezdrátových sítí

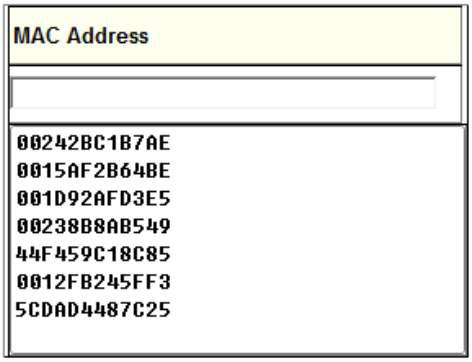
6.1.1 Skrytí SSID

Skrytí SSID je nejjednodušší zabezpečení, ale dnes také nejlépe prolomitelné. Útočníkovi se nezobrazí síť v seznamu dostupných bezdrátových sítí, ale například s pomocí programu NetStumbler ji může odhalit. SSID sítě je volně přenášeno, proto lze jednoduše zachytit.

6.1.2 Kontrola MAC adresy

Patří mezi pokročilejší zabezpečení sítě. Na přístupovém bodu se nastaví seznam MAC adres klientů, kteří mají dovoleno připojit se. Ostatním klientům je přístup odmítnut.

Útočníkovi však stačí chvíli monitorovat komunikaci a tím zachytit povolenou MAC adresu. Poté již stačí změnit MAC a vystupovat za oprávněného útočníka.



Obrázek 6.1: Seznam povolených MAC

6.1.3 Pravidla pro WEP

V dnešní době je WEP zabezpečení již příliš nebezpečné a nedoporučuje se jej používat. U tohoto protokolu nám nepomůže ani silné heslo. Pro prolomení stačí zachytit dostatečné množství inicializačních vektorů.

6.1.4 **Pravidla pro WPA2**

Útoky na WPA spočívají v zachycení tzv. „handshaku“. Jakmile je odchycen samotný útok již může být prováděn mimo bezdrátovou síť. Prvním druhem útoku je slovníkový útok, kde se porovnává šifrované heslo. Tento útok využívá databázi známých hesel k porovnávání zachyceného. Druhým typem útoku je útok hrubou silou (brute-force).

Nejlepší obranou proti slovníkovému útoku je použití nestandartního hesla, které není lehké odvodit. To zvětší šanci, že námi zvolené heslo nebude obsažené v databázi hesel dostupné na internetu.

To samé platí pro útok hrubou silou, kde se uplatňuje vypočtení výkon počítače k dešifrování hesla. Uživatelé by proto měli dodržovat zásady tvorby hesla, kdy se použijí znaky a-z, A-Z, 0-9 a speciální znaky. Takto vytvořené heslo mnohonásobně zvyšuje nemožnost prolomení.

Pro znemožnění útoků na síť použitím slovníkového a brute-force útoků se do podnikových sítí implementuje RADIUS server, který nám zajišťuje dostatečné zabezpečení.

7 Praktická implementace navržených metod zabezpečení

7.1 Intrusion Detection Systems (IDS)

Jedná se o bezpečnostní nástroje počítačových sítí, které se začaly používat v druhé polovině devadesátých let minulého století. IDS je obranný systém, který monitoruje síťový provoz a snaží se pomocí zdrojů, metod a nástrojů identifikovat a hlásit neschválené či neautorizované aktivity. Základní podstatou těchto nástrojů spočívá, že dokáží rozeznat činnost narušitele od činnosti běžného uživatele pomocí identifikátorů. Systém sám o sobě nedokáže zabránit narušení, ale dokáže upozornit a varovat před potencionálním narušením.

7.1.1 Metody detekce

Detekce vzoru

Systém používá porovnávání datového provozu na síti s databází signatur známých útoků. Jedná se o jednoduchou metodu, která je přesná. Nevýhodou je, že je závislá na existenci podpisu daného útoku v databázi.

Dekódování protokolu

Systém rozezná použitý protokol komunikace mezi entitami a aplikuje pravidla definovaná v RFC (Request for Comments). Následně hlásí případné porušení pravidel.

Detekce anomálií

Systém detekuje odchylky od normálního provozu sítě. Problém této metody je určit, co je normální chování sítě. Často se využívají algoritmy umělé inteligence, např. neuronové sítě. Při jakýchkoliv odchylkách v provozu sítě IDS detekuje tyto změny a generuje alarm. Je obtížné rozhodnout, zda se jedná o útok nebo typický provoz. Výhodou systému je případná detekce nového, neznámého útoku.

V reálném provozu se obvykle využívají kombinaci více detekčních metod. Odpovědí IDS na útok může následně být reset podezřelého spojení, zahájení filtrace nebezpečného provozu na směrovači a záznam podezřelé aktivity. V těchto případech IDS pomocí IPS nejen monitoruje, ale i aktivně chrání prvky počítačové sítě a koncové stanice před důsledky případných útoků.

7.1.2 Kategorie IDS

Systémy detekce průniku se řadí do dvou kategorií:

Uzlově orientované systémy (hostbased intrusiondetection systems, HIDS)

Síťově orientované systémy (networkbased intrusiondetection systems, NIDS)

Uzlově orientované systémy

Softwarový balíček nainstalovaný na koncové stanici, který monitoruje a vyhodnocuje lokální aktivity. Využívá se logovacích souborů a sleduje se v nich, zda nedochází k významným a podezřelým změnám. Kontrola se provádí pouze na koncové stanici.

Síťově orientované systémy

Jedná se o samostatné zařízení či program, které monitoruje síťový provoz na něj svedený. Senzory bývají většinou umístěny přímo na síťových prvcích (hub, switch) a zachytávají tak veškerý provoz. Z následné analýzy provozu poté upozorňuje na možné problémy a incidenty u jiných koncových stanic

7.2 Snort

Snort se řadí do kategorie softwarových síťových IDS, založených na pravidlech. *Snort* monitoruje provoz sítě a detekuje potenciální útoky. Hledá vzorky známých útoků a v případě nalezení je schopen provádět různé úkony, avšak probíhající provoz nepřerušuje. Program *Snort* je vyvíjen pro řadu platforem, tak není problém jej používat jak na Unixových systémech, tak na systému Windows.

Režimy Snortu:

- Sniffer mode – V tomto módu zachytává pakety (sniffuje) a zobrazuje je uživateli.
- Packet logger mode – Rozšíření sniffer mode, zachycená data se zapisují do logovacích souborů.
- Network Intrustion Detection System – Nejvýznamnější režim, odchycená data porovnává s uživatelem definovanými pravidly.
- Inline – V tomto módě pracuje jako HIDS. Pakety získává z iptables. Na základě pravidel rozhoduje o zahození nebo povolení paketů.

Nejdůležitější části *Snortu* je detekční jednotka. Úkolem detekční jednotky je, porovnávaní dat uvnitř každého paketu. Zkontroluje, zda neobsahuje řetězec, který vyhovuje definovaným pravidlům. Jestli obsahuje shodu, vyvolá uživatelem definovanou akci, a to zápis do logu či vyvolaní výstrahy. Tento module je náročný na výkonu počítače, může dokonce vést, při zatížení sítě k zahazovaní paketů. Zatížení jednotky závisí na následujících faktorech:

Nejdůležitější částí *Snortu*, kterou je nutné zmínit je „detekční jednotka“. Slouží k porovnávání dat uvnitř každého paketu a kontroluje, jestli tento paket vyhoví definovaným pravidlům, poté následuje nastavená akce uživatelem, a to buď výstraha nebo zápis do logu v „tcpdump“ tvaru. Všechny logy se implicitně ukládají do adresáře /var/log/snort. Tento modul *Snortu* je výpočetně náročný a vytížení procesoru záleží na následujících faktorech:

- Počet pravidel
- Výkon počítače
- Rychlost vnitřní sběrnic
- Zatížení sítě

Důležitou vlastností *Snortu* je možnost vytváření a přidávaní vlastních pravidel. Díky tomu můžeme přizpůsobit pravidla potřebám naší sítě.

Obecný tvar pravidla Snortu:

```
akce protokol zdroj_ip zdroj_port směr cíl_ip cil_port (volby)
```

Každé pravidlo se skládá ze dvou částí: hlavičky a volby. Hlavička obsahuje akci, která se má vykonat (alert, log, pass), protokol, zdrojová a cílová adresa s porty. Volby tvoří srdce IDS *Snortu*. Pomocí voleb můžeme vytvořit popisnou zprávu a kontrolovat různé atributy paketů.

Příklad jednoduchého pravidla:

```
log udp any any -> 192.168.1.0/24 1:80
```

Snort zapíše záznam UDP paketu z jakékoliv adresy a portu směřujícího na adresu sítě 192.168.1.0/24. Cílový port je v rozsahu od 1 do 80.

7.3 RADIUS

V této kapitole je popsán nástroj pro zabezpečí bezdrátové sítě pomocí RADIUS serveru, sloužící k ověření uživatele a chránící před útoky na síť využívající PSK klíč.

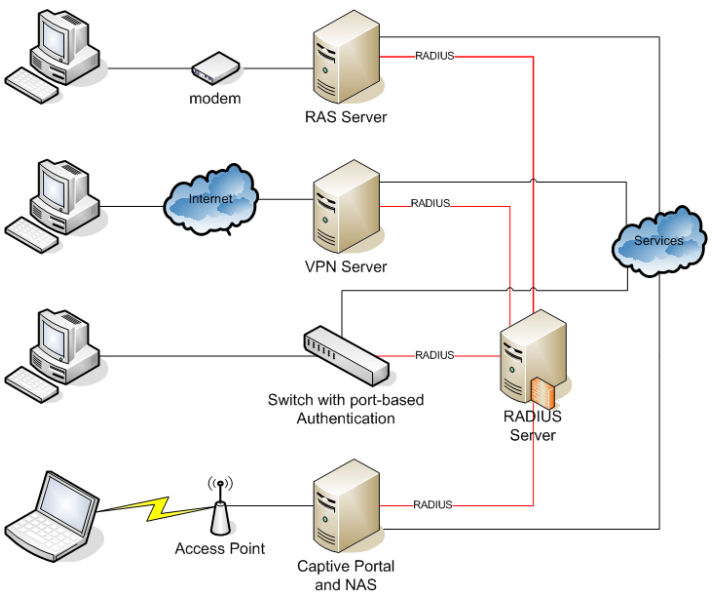
RADIUS (Remote Authentication Dial In User Service, česky: Uživatelsky vytáčená služba pro vzdálenou autentizaci) je síťový protokol, který poskytuje centralizované ověřování, autorizaci a správu účtu (AAA). Je určen pro správu připojení. Používá se jako síťová služba. RADIUS byl vyvinut firmou Livingston Enterprises, Inc. v roce 1991 jako protokol k ověření přístupu s autentizací a správou účtů. Byl zařazen mezi normy IETF (RFC dokument 2865).

Vzhledem k široké podpoře protokolu RADIUS, je často používán poskytovateli internetových služeb a podniků k řízení přístupu na internet nebo vnitřní sítě, bezdrátové sítě a integrované e-mailové služby. Tyto sítě mohou zahrnovat modemy, DSL, přístupové body, VPN, síťové porty, webové servery, atd.

RADIUS je klient / server protokol, který běží v aplikační vrstvě, pomocí UDP protokolu. RAS, VPN a NAS, jsou brány, které řídí přístup k síti a všichni mají klienta RADIUS, který komunikuje s RADIUS serverem. RADIUS server je obvykle proces běžící na pozadí systému UNIX nebo Windows NT.

Tři funkce RADIUS:

- K ověření uživatele nebo zařízení před poskytnutí přístupu k síti.
- Povolit tyto uživatele nebo zařízení pro síťové služby.
- Správu těchto služeb.



Obrázek 7.1: Schéma RADIUS serveru

7.3.1 Autentizace a autorizace

Autentizace znamená ověření pravosti. Autentizace patří k bezpečnostním opatřením a zajišťuje ochranu před falšováním identity, kdy se subjekt vydává za někoho, kým není. Rozlišujeme autentizaci entity (osoby, programu) a autentizaci zprávy.

Autorizace je oprávnění, schválení, pověření. Proces autorizace označuje získání přístupu k informacím, funkcím a dalším objektům. [35, 36]

Uživatel nebo zařízení odešle žádost Network Access Server (NAS) k získání přístupu k síťovému prostředku pomocí zvláštního pověření. Pověření jsou předávány do zařízení NAS přes Point-to-Point Protocol (PPP).

Na druhé straně, NAS odešle zprávu s žádostí o přístup RADIUS serveru, o povolení k poskytování přístupu přes RADIUS protokol. Tato žádost obsahuje přístup, obvykle ve formě uživatelského jména a hesla nebo bezpečnostního certifikátu poskytnutého uživatelem. Dále může obsahovat další informace, které NAS ví o uživateli, jako je jeho síťová adresa nebo telefonní číslo.

RADIUS server ověří správnost informací pomocí autentizace schémat jako PAP, CHAP nebo EAP.

Pokud je uživatelské jméno a heslo přijato, server autorizuje přístup k poskytovateli internetu a vybere IP adresu (popřípadě rozsah adres) a další parametry spojení, což mohou být např. L2TP přihlašovací údaje, doba po kterou může být uživatel připojen, rychlost připojení, kterou může uživatel používat, nebo jiná omezení. RADIUS protokol neposílá hesla mezi NAS a RADIUS serverem v čistém textu (ani při použití s PAP protokolem), používá se MD5 hašování.

Moderní RADIUS servery můžou odkazovat na externí zdroje - SQL, Kerberos, LDAP nebo Active Directory - pro ověření uživatele.

7.3.2 Instalace RADIUS server

Instalace

Produkt je v dostání pod GNU licencí. Existuje mnoho balíčků s odlišností na použitý systém. Veškeré podrobné informace jsou dostupné na stránkách

http://freeRADIUS.org.

Instalace RADIUS serveru.

```
sudo apt-get install freeradius-mysql
```

Tímto máme nainstalovaný FreeRADIUS s podporou MySQL. Zbývá jen nakonfigurovat tyto servery a vytvořit spojení, aby mohly spolu komunikovat.

Konfigurace

Zvláštní odstavec je věnován popisu prostředí a několika konfiguračním souborům, kterým nevyhneme. Na různých počítačích se nacházejí konfigurační soubory v různých adresářích. Často je tato adresa */etc/raddb*, nebo */etc/freeradius*.

users - Tento soubor slouží jako jednoduchá databáze uživatelů. My jej potřebovat nebudeme, ale je velmi vhodné se do tohoto souboru podívat. Je dobře okomentovaný a jsou v něm příklady záznamů uživatelů.

radiusd.conf - Soubor s hlavní konfigurací serveru. Pro nás je důležité, že mimo jiné specifikuje, jaké postupy zvolit při žádostech o autentizaci a autorizaci. Dnes je tento soubor rozdělen do několika souborů jako je */sites-enabled/inner-tunnel, default, modules/ aj.*

sql.conf - Velmi důležitý soubor. Definuje kde se nachází SQL (implicitně MySQL) databáze a jak z ní dostat všechny potřebné informace. Jsou zde definovány SQL dotazy. Je vhodné pročíst si komentáře.

clients.conf - Soubor definující povolené přípojné body NAS. Nemá-li NAS záznam v tomto souboru pak s ním FreeRADIUS nekomunikuje. Výjimkou je, pokud je uveden v SQL databázi a FreeRADIUS je nakonfigurován, aby se do ní díval. My si toto vyzkoušíme. Implicitně je zde definován NAS localhost.

Testování

Dříve než začneme je potřeba FreeRADIUS server nejdříve ukončit a poté spustit v debugging módu.

`sudo /etc/init.d/freeradius start|restart|stop` - nastartuje službu `freeradius -X stdout` - spuštění samotného RADIUS serveru v debugging módu s podrobným vypisováním logu na obrazovku

`sudo /usr/sbin/freeradius -X | more` – podrobnější výpis, než samotné -X

```
 attr_filter attr_filter.accounting_response {
       attrsfile = "/etc/freeradius/attrs.accounting_response"
       key = "%{User-Name}"
 }
Module: Checking session {...} for more modules to load
Module: Checking post-proxy {...} for more modules to load
Module: Checking post-auth {...} for more modules to load
}
radiusd: #### Opening IP addresses and Ports ####
listen {
       type = "auth"
       ipaddr = *
       port = 0
}
listen {
       type = "acct"
       ipaddr = *
       port = 0
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on proxy address * port 1814
Ready to process requests.
```

Obrázek 7.2: Spuštění RADIUS

Pro testování lze použít program `radtest` nebo `radclient` se zapnutým debugováním. Nezapomeňte, že po každé změně konfiguračního souboru, je nutné FreeRADIUS ještě restartovat.

Konfigurace FreeRADIUS serveru

Nyní se již dostáváme ke konfiguraci FreeRARIUS serveru. Začneme souborem *sql.conf*, ve kterém musíme doplnit údaje o tom, kde se nachází naše databáze, přístupové uživatelské jméno a heslo.

```
# Connect info
 server = "adresa_serveru"
 login = "uziv_jmeno"
 password = "heslo"
   radius_db = "nazev_databaze"
```

Poté je nutné nakonfigurovat server, aby věděl, že má ověřovat požadavky pomocí SQL. Toto nastavení se mění v souboru */sites-enabled/inner-tunnel, default* (*radiusd.conf* ve starší verzi), (ta část, která nás zajímá se nachází ke konci tohoto souboru). Ujistěte se, že v bloku *authorize* máte nezakomentovanou řádku s sql:

```
authorize {
        preprocess
        chap
        mschap
        #attr_filter
        #eap
        suffix
        sql
        #files
}
```

Se zakomentovaným *files* server nebude hledat údaje v souboru *users*.

V bloku *authenticate*:

```
authenticate {
 authtype PAP {
 pap
 }
 authtype CHAP {
 chap
 }
 authtype MS-CHAP{
 mschap
 }
      #digest
 #pam
 #unix
 #authtype LDAP {
 # ldap
 #}
}
```

V části *accounting* odkomentujeme *sql*:

```
preacct {
      acct_unique
 preprocess
 suffix
 #files
}

accounting {
 detail
       #unix
 sql
 #radutmp
 #sradutmp
}
```

Zbytek souboru *inner-tunnel, default* (*radiusd.conf*) ponecháme zatím beze změn.

8 Závěr

Hlavní náplní diplomové práce bylo vytvořit monitorovací systém bezdrátové sítě Honeypot a poté analýza zachyceného provozu. Díky monitorovacímu systému jsme schopni včas odhalit probíhající útok, který útočník provádí a ihned zakročit nebo zpětně zjistit způsob útoku na naší síť. Následnou analýzou provozu můžeme realizovat různé bezpečnostní opatření k navýšení zabezpečení sítě. Z provedené analýzy jsem zjistil, že útok na naší bezdrátovou síť byl jen ojedinělý a už se neopakoval. Dále bylo prokázán, již známý fakt, že protokol WEP je nedostatečný způsob ochrany a jeho prolomení je jen otázka minut s minimální námahou a nároky na hardware. Proto by se ho uživatelé, správci WLAN sítí měli vyvarovat jeho nasazení. Pro domácí sítě nám zcela dostačuje použití WPA protokolu, který nám zajišťuje dostatečné zabezpečení. Nejlepší možnou ochranou sítě je implementace RADIUS serveru. Z důvodu zakázání komunikace vyjma provozu 802.1x, činní klasické útoky na síť zcela nepoužitelné. Útoky typu DoS jsou snadno zjistitelné, ale ochrana proti nim je náročná. Možnou variantou ochrany je použití kombinace IDS a IPS systémů, který dokáže tento útok detekovat a popřípadě zablokovat komunikaci.

Rozšiřujícím prvkem a následným vývojem této práce je možnost simulování služeb a jejich monitoring. Nebo použití služeb Honeypot i v jiných oblastech sítí například VOIP.

9 Seznam obrázků

Použitá literatura

[1] BARKEN, Lee. *Wi-Fi*: *jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004, 174 s. ISBN 80-251-0346-3.

[2] ZANDL, Patrik. *Bezdrátové sítě WiFi Praktický průvodce.* Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-7226-632-2.

[3] JOSHI, R. C. SARDANA, Anjali. *Honeypots: A New Paradigm to Information Security* Vyd. 1. Enfield: CRC Press, 2011, 328s. ISBN 978-1578087082.

[4] HORÁK, Jaroslav, KERŠLÁGER, Milan. *Počítačové sítě pro začínající správce* Vyd. 4. Brno: Computer Press, 2008, 328 s. ISBN 978-80-251-2073-6

[5] MILLER, S. Stewart. *WiFi security* Vyd. 1. New York: McGraw-Hill Professional, 2003, 309s. ISBN 978-0071410731.

[6] LEHEMBRE, Guillaume. *Bezpečnost Wi-Fi: WEP, WPA a WPA2*. 2006, s. 14. Dostupné z: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf

[7] Honeyd. [online]. [cit. 2012-05-03]. Dostupné z: http://www.honeyd.org/index.php

[8] [online]. [cit. 2012-05-03]. Dostupné z: http://www.symantec.com/connect/articles/wireless-honeypot-countermeasures&usg=ALkJrhhTmf0PsrW-08cuemPnGPx3-smq9g

[9] KFSensor. [online]. [cit. 2012-05-03]. Dostupné z: http://www.keyfocus.net/kfsensor/

[10] Honeypot. [online]. [cit. 2012-05-03]. Dostupné z: http://www.security-portal.cz/clanky/tvorime-honeypoty

[11] ORKÁČ, Radomír. IDS SnortIDS Snort. 2006, s. 22. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/projekty0506/Snort.pdf

[12] DAŘÍLEK, Martin. Standardy 802.11e a 802.11i. s. 11. Dostupné z: http://www.cs.vsb.cz/grygarek/TPS/projekty/0506Z/tps_dar022.pdf